TELECOM INFRA PROJECT

Open Core Network Project Group

Applications and Services

Technical Requirements v1.0

Authors:

- **Phil Ritter, Facebook**

Contributors:

- **Sagiv Draznin, Rakuten**
- **Veronica Quintuna-Rodriguez, Orange**
- **Marc Price, Matrixx**
- **Sergio Tarazona, Entel Peru**
- **Tassos Michail, Facebook**

Editors:

- **Chris Morton, Isn't That Write**

Change Tracking

Date	Revision	Author(s)	Comment
March 11, 2020	v0.1	Tassos Michail	Initial template
March 20, 2020	v0.1a	Phil Ritter	Added objectives
May 25, 2020	v0.2	Phil Ritter	Merged MVC use cases and requirements into single document. General reorg of chapter flow. Added requirements.
Jun 26, 2020	V1.0	Phil Ritter	Cleaned up formatting. Added references on requirements. Added requirements based on feedback from WS 1 team member.
June 30, 2020	V1.01	Phil Ritter	Added performance requirement section.
July 20, 2020	V1.02	Phil Ritter	Updated to add references to CHF. Added placeholder sections for reliability, availability and restart. Minor editorial updates.
July 31, 2020	V1.03	Phil Ritter	Updated with inputs from Sergio Terazona from Entel. Also minor editorial updated.
August 12, 2020	V1.04	Veronica Quintuna	Added glossary items Terminology comments/suggestions. Minor editorial updated.
Sept. 19, 2020	V1.05	Chris Morton	Cleaned up formatting. Proofreading and line editing. Minor editorial revising. Continuity checking. Checked conformance with (US) Plain Writing Act of 2010. Revised graphics captioning.

Table of Figures

1. Introduction

This document describes technical requirements for network function applications and services of an open core network (OCN) implementation. It describes the necessary software functions, and the requirements that the implementation needs to meet to be deployed in the networks of the specific operators participating in this specification.

1.1. Why Open Core

The Open Core Network Group is working to develop an open, cloud-native, and converged core that is a collection of microservices implementing various core network functions (open, flexible, and extensible):

- Runs on standardized software and hardware infrastructure (i.e., infrastructure agnostic)
- Supports 3GPP 5GC and 4G EPC (licensed), Wi-Fi (unlicensed), and shared spectrum (e.g., CBRS) networks (i.e., access agnostic)
- Enables seamless migration from 4G EPC to 5GC in both non-standalone (NSA) and standalone (SA) modes.
- We do not intend to support legacy access modes (no 2G or 3G access support).

The goal is to innovate on packet core technologies across any access wireless networks operating on licensed, unlicensed, and shared spectrum; develop microservice, orchestration, and automation frameworks on OCN platform; and support an ecosystem of developers, OEMs, SIs, MNOs, and ISPs around OCN-based solutions.

1.2. Document Scope

This document aims to:

- describe the architecture and software requirements of a 5G minimum viable core (MVC)
- specify the required core network functions of a 5G MVC
- specify the cloud environment requirements for OCN deployment
- define the core network function requirements and decomposition into OCN microservices

A separate, detailed, low-level technical requirement specification (TRS) will be developed in parallel for each workstream as part of the software project.

1.3. Document Structure

This document is structured as follows:

- Chapter 1: Introduction
- Chapter 2: Open Core Network Architecture
- Chapter 3: Open Core Use Cases and MVC
- Chapter 4: Open Core Application and Services Functional Requirements
- Chapter 5: Glossary

2. Open Core Network Architecture

The OCN goal is to implement a multi-access converged core supporting 5G and 4G RANs as specified by 3GPP in addition to non-3GPP access methods including Wi-Fi and fixed line services. This development will be staged in releases:

- A 5G MVC delivering basic functionality of 5G targeting limited use cases,
- Full 5GC core (F5GC) delivering the essential capabilities of a 5G standalone, service-based architecture (SBA) core as specified by 3GPP
- A converged core (CC) delivering 5G-SA with support for additional 3GPP (4G) and non-3GPP (Wi-Fi) access methods.

2.1. 5G Minimum Viable Core (MVC)

The OCN MVC core will deliver the minimal set of network functions required to support one or more specified MVC limited use cases. These use cases are described in chapter 3 of this document. The MVC core may deliver a subset of the full 3GPP reference point interfaces that is required support the limited use case (e.g., the N4 interface may not implement all procedures necessary to support handover and mobility when the fixed wireless access use case is implemented).

At a minimum, the OCN MVC Core shall support:

- The UPF, AMF and SMF network functions, with limited capability as required for the MVC use case.
- The 3GPP reference point interfaces facing the 5G RAN, including N1, N2 and N3, with limited capabilities as required to support the MVC use case.
- The 3GPP reference point interface, N6, facing the data network.

Other network functions specified as part of the full 5G-SA core may be delivered as required to support the MVC use case, in some cases in a highly simplified form providing minimal capability as required to complete certain call flows and make the MVC functional.

2.2. Full 5G-SA SBA Core (5GC)

Building on the MVC, the next goal of OCN is to deliver a full 5G Stand Alone core network suitable to support multiple deployment scenarios and use cases. The full 5G-SA core will support all major functions of the 5G core as defined by 3GPP in TS 23.502. The full 5G-SA SBA core consists of the following network functions:

UPF – User Plane Function

SMF – Session Management Function

AMF – Access and Mobility Function

AUSF – Authentication Server Function

UDM – User Data Manager

PCF – Policy Control Function

NRF – Network Resource Function

NEF – Network Exposure Function

NSSF – Network Slice Selection Function

AF – Application Function

CHF – Charging function

Detailed descriptions of each network function and its relevant procedures and interfaces can be found in ETSI TS 23.502.

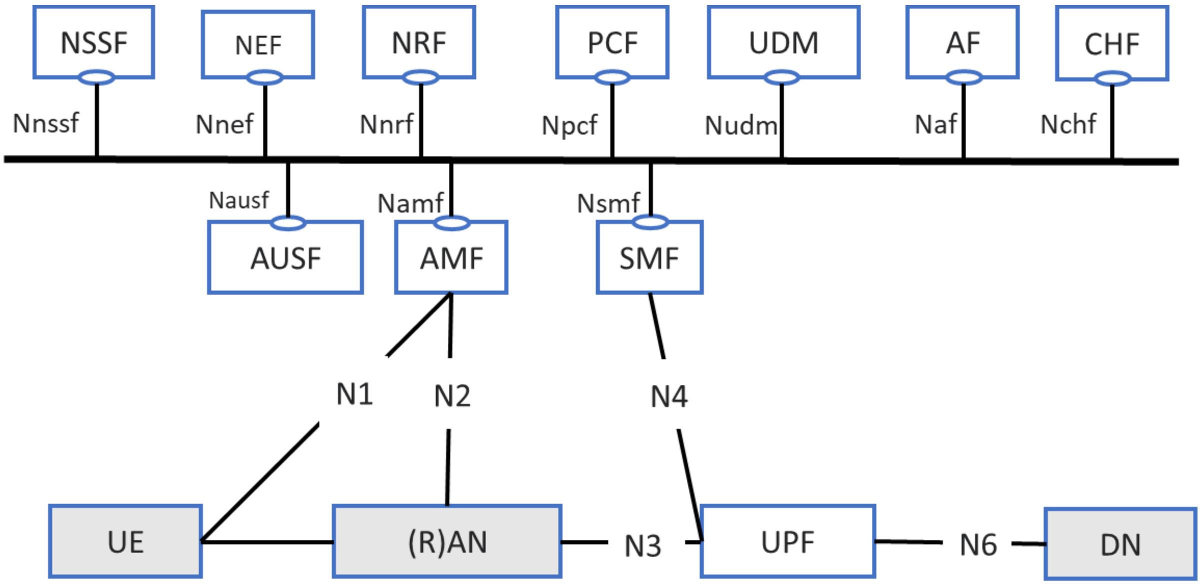

Figure 1 – 3GPP 5G-SA SBA architecture

OCNs implementation of the full 5GC core shall be interoperable with non-OCN 5GC components on the 3GPP reference point interfaces.

2.3. Converged Core (CC)

Ultimately, OCN plans to deliver the 5G core with integration of non-5G access methods, including 3GPP standard 4G-LTE and non-3GPP access methods such as Wi-Fi or wired access methods. The OCN project goal is to implement GSMA Option 4, with both the 5G "new radio" base stations (5G-NR) and the 4G-LTE base stations (eNodeB) under the control of the 5G core and no requirement for a separate 4G EPC.

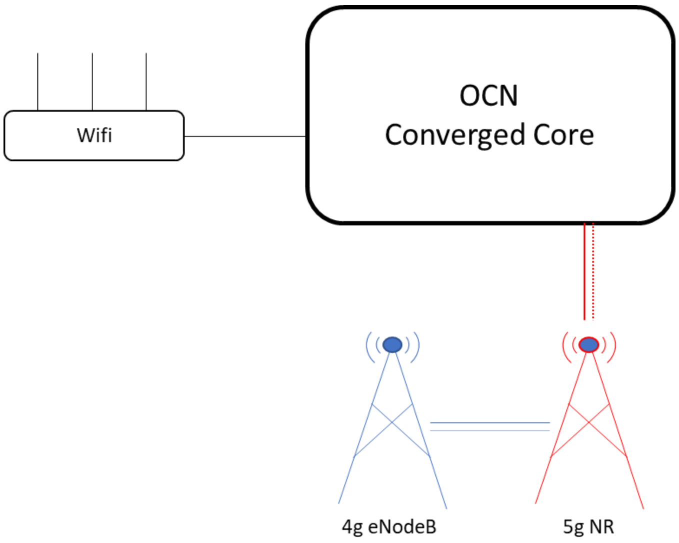

Figure 2 – OCN converged core

3. Open Core Use Cases and MVC

3.1. MVC Use Cases

3.1.1. Fixed Wireless 5G

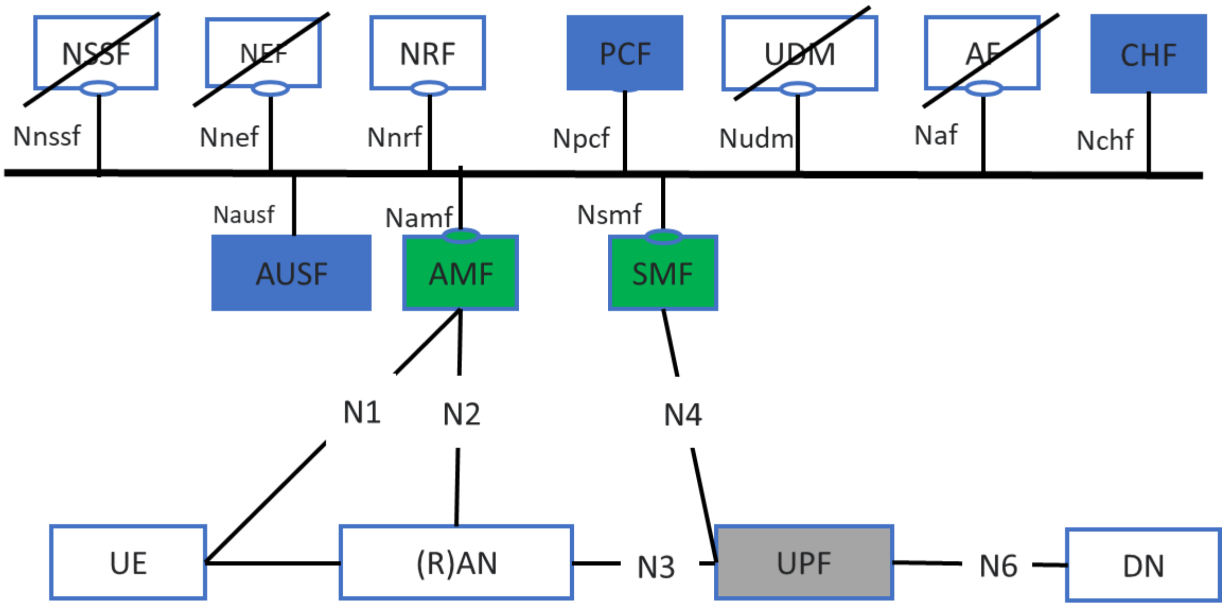

Figure 3 – Fixed wireless 5G

Provide a 5G-SA core for the purpose of providing fixed wireless services. This application has the following characteristics:

- Assumes that UE will be dedicated gateway device that uses the 5G network as an ISP-like access method and provides in-home or in-office services by bridging to Wi-Fi, wired or other local area network methods
- May include specialized advanced services in the gateway, e.g., VoIP, video, or personal assistant.
- Does not require mobility. Once a session is attached the UE does not move. If a session is dropped or a mobility event is detected (due to RAN fault or change in RF conditions) the UE can simply reattach
- Authentication and authorization functions can be simplified. May use standard UICC validating to AUSF/UDM but because it is a “closed” system with dedicated UEs, other authentication methods can be considered to simplify development
- Policy control function (PCF) is not in scope but an interface to PCF should be developed in the initial MVP. This stub-PCF function can be supplied to terminate the Npcf refence point but its responses may be simple constant responses.
- Charging function (CHF) is not in scope but an interface to CHF should be developed in the initial MVP. A stub-CHF shall enable simple CDR creation for network usage, although the interface can be improved later to support converged charging following 3GPP standards.
- No specialized applications are provided by the core – just connectivity to data network, most likely direct to internet

High level requirements:

- UPF: Basic session attach
- UPF: Requires basic firewall (FW) functionality. If FW rules are global (not user specific) then may be handled outside UPF by FW appliance
- UPF: Requires CG-NAT as large inventory of public IP likely unavailable. May be able to handle NAT external to UPF by NAT appliance
- UPF: Requires significant performance to handle typical fixed ISP bandwidth (speeds/feeds to be specified)
- UPF/SMF: IPv4 user sessions required, IPv6 support highly desired
- SMF: Basic session management – attach, detach
- AMF: Minimized to support attach, detach and session maintenance procedures only. No mobility
- AMF: Requirement for N1 interface needs to be investigated/confirmed. May not need
- AUSF: Basic authentication and authorization procedures only
- UDM: Not required
- PCF: Minimum functionality. Required only to respond to mandatory procedures during attach/detach
- NRF: Minimal functionality. Could be supplied using fixed DNS
- NEF: Not required
- NSSF: Not required
- AF: No dedicated AF required. DN is public internet

Other considerations and potential requirements:

- May need to provide support for LI functions, depending on regulatory requirements in the market/country of deployment
- Charging function (CHF) is not in scope but an interface to CHF should be developed in the initial MVP. Initially, simple CDR creation should be possible for network usage, although the interface can be improved later to support session-based charging and location/registration charging following 3GPP standards for interfacing SMF and AMF respectively
- Possible support of application function for private services provided to customers (i.e., video services)

Services required:

- CG-NAT (unlikely that sufficient public IP addresses are available to support all connected devices)
- Basic firewall
- Simple DPI/app detection
- Possibly LI, if deployed in jurisdiction where required
- Others TBD

3.1.2. Private 5G

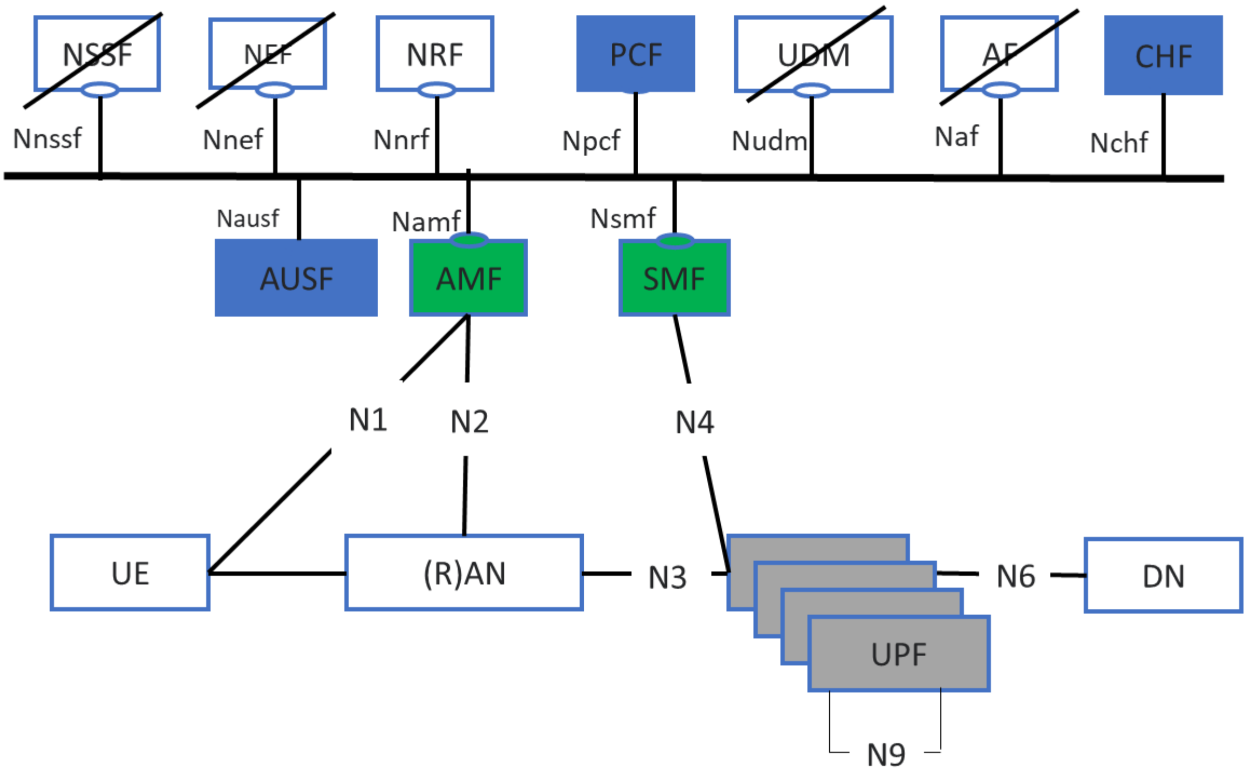

Figure 4. Private 5G

Private 5G is the deployment of a self-contained 5G core and associated RAN elements to support a closed user group. Typically thought to be an enterprise deployment of 5G using either licensed or unlicensed (CBRS) spectrum for the enterprise's exclusive use with a factory, office complex or localized outdoor environment (e.g., an oilfield or similar industrial facility). Most community discussion of private 5G focuses on IoT applications (factory automation/sensors, oilfield automation, etc.) but more generic use cases could be in scope.

- Mobility depends upon actual use case. May not be required for IoT/factory automation but more generic use cases could need it. When not required, if a session is dropped or a mobility event is detected (due to RAN fault or change in RF conditions) the UE can simply reattach
- Authentication and authorization functions can likely be simplified
- Specialized applications may be provided, e.g., factory automation apps
- Some use cases may require attention to latency, in which case policy based QoS control may be required

High level requirements:

- UPF: Basic session attach
- UPF: May require implementation of QoS enforcement, queues, and rate limits
- UPF: Requires basic firewall functionality
- UPF: CG-NAT may not be required if closed/private IP allocation is sufficient
- UPF/SMF: IPv4 only operation likely enough
- SMF: Basic session management – attach/detach
- SMF: May be required to support QoS features
- AMF: Minimized to support attach, detach and session maintenance procedures only. No mobility
- AMF: May be required to support QoS features

- AMF: Requirement for N1 interface needs to be investigated/confirmed. May not need.
- AUSF: Basic authentication and authorization procedures only.
- UDM: Basic authentication procedures only.
- PCF: May be required to support QoS features
- NRF: Minimal functionality. Could be supplied using fixed DNS
- NEF: Not required
- NSSF: May be required if deployment requires support for low-latency or high-reliability services
- AF: Possibly required depending on specific use case.

Other considerations and potential requirements:

- LI functions not required for fully private deployments in most world jurisdictions (if no interconnect with public internet)
- Charging function (CHF) is not in scope but a stub-nCHF interface to CHF should be included as a first step. The interface can be developed later to support session-based charging and location/registration charging following 3GPP standards for interfacing SMF and AMF, respectively.
- Possible support of application function for IoT/automation features
- Ultra-low latency may be required for some factory or process automation applications

Services required:

- Basic firewall
- Simple DPI/app detection may be needed if enterprise security/policy enforcement is required
- LI only required if private services are bridged to internet and required by local jurisdiction regulation
- Others TBD

3.1.3. Private 5G Integrated with Service Provider Control

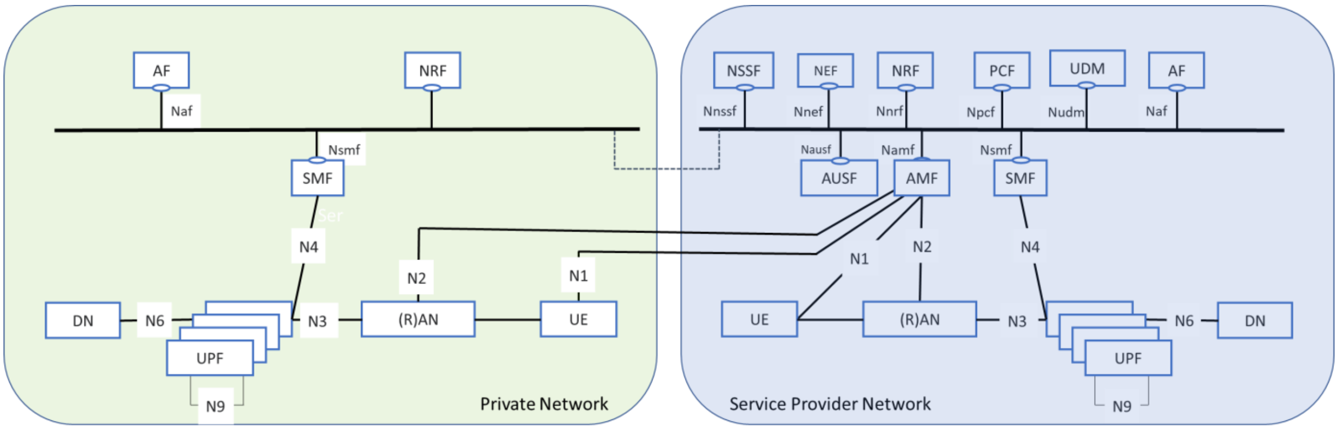

Figure 5 – Service provider managed private 5G

Private 5G with service provider control is the deployment of a self-contained or public-shared 5G RAN and limited 5G core functions (typically SMF/UPF only). Primary 5G core functions are provided by a public 5G service provider (e.g., MNO).

In some cases, network slicing functions may be used on the private RAN assets to allow the service provider to provide shared service using the private RAN. Typically, this use case allows the private enterprise to deploy RAN to cover "in building" within their offices/factories or other sites allowing the integrated Service Provider to manage the network on their behalf.

- The following functions are hosted by the enterprise: UPF, SMF, local DN and possibly AF(s)
- The following functions are provided by the service provider/MNO: AMF, AUSDF, UPF, NSSF, NRF and NEF
- The PCF may be provided by the enterprise, service provider or possibly both depending upon specific use case
- Mobility is generally required, but the mobility functions of the AMF are supplied by the service provider. the enterprise SMF would require mobility procedures
- Authentication and authorization functions are provided by the Service Provider
- Specialized applications may be provided, e.g., factory automation apps
- Some use cases may require attention to latency, in which case policy based QoS control may be required

High level requirements:

- UPF: Basic session attach
- UPF: May require implementation of QoS enforcement, queues, and rate limits
- UPF: Requires basic firewall functionality
- UPF: CG-NAT may not be required if closed/private IP allocation is sufficient inside the enterprise DN
- UPF/SMF: IPv4 only operation likely enough. Network operator may desire support of IPv6
- SMF: Basic session management and mobility functions required
- SMF: May be required to support QoS features
- AMF: *Provided by the service provider*
- AUSF: *Provided by the service provider*
- UDM: *Provided by the service provider*

- PCF: Typically *provided by the service provider*, but local QoS use cases may require

PCF for private network with support for QoS functions

- NRF: *Provided by the service provider*
- NEF: *Provided by the service provider*
- NSSF: *Provided by the service provider*
- AF: Possibly required depending on specific use case

Other considerations and potential requirements:

- LI functions likely required, under the control of the service provider (Xn interface procedures required on SMF and UPF, with LI functions deployed by service provider)
- Charging function (CHF) is not in scope but an interface to CHF should be developed in the initial MVC. Initially, simple CDR creation should be possible for network usage, although the interface can be improved later to support session-based charging and location/registration charging following 3GPP standards for interfacing SMF and AMF respectively
- Possible support of AF for private enterprise services

Services required

- Basic firewall
- Simple DPI/app detection may be needed if enterprise security/policy enforcement is required
- LI only required if private services are bridged to internet and required by local jurisdiction regulation
- Others TBD

3.1.4. MEC UPF

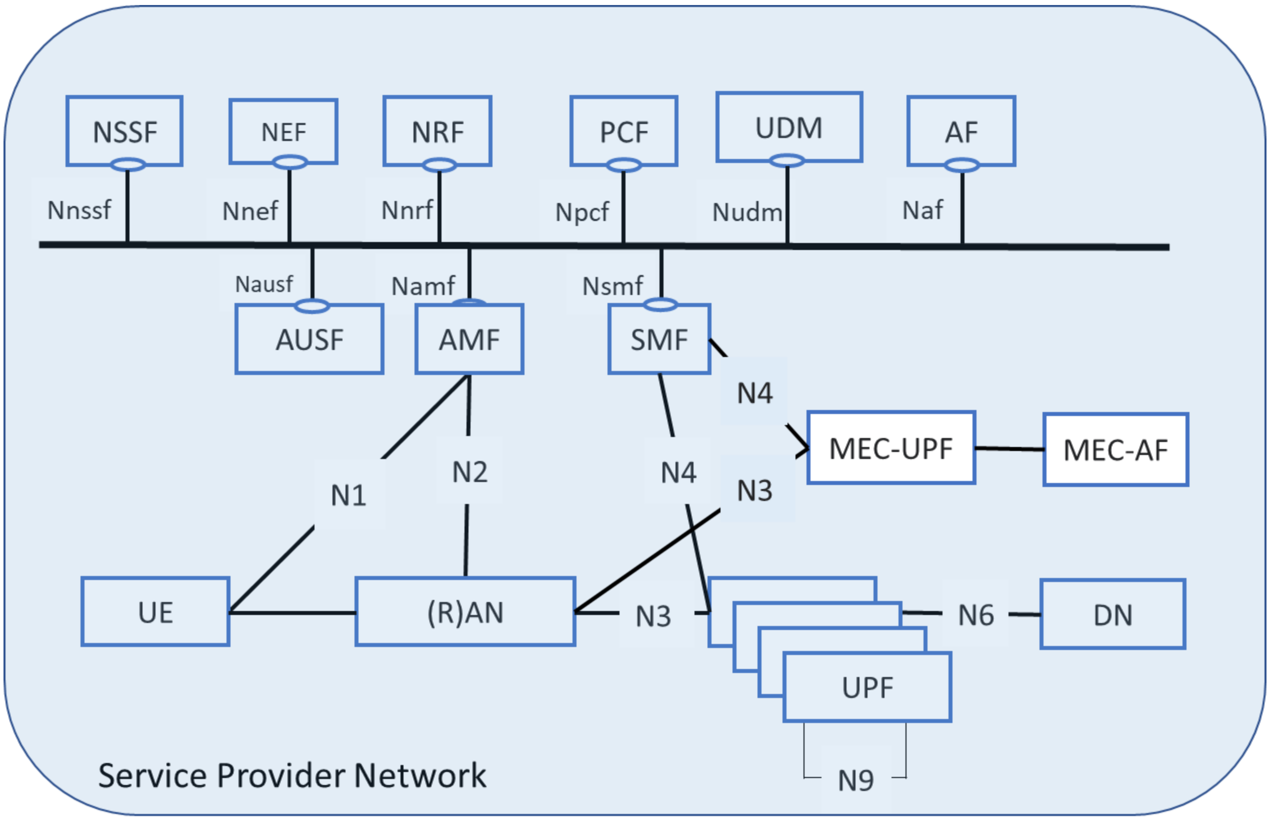

Figure 6 – MEC UPF

Local UPF for support of MEC functions at the local breakout site. The TIP/OCN UPF could be deployed as a standalone network function to serve this use case.

- The UPF function can be highly simplified, limited to specific capabilities required by the edge compute application
- UPF would function under the control of 5G core provided by a service provider
- The UPF network function could be deployed as a software module embedded into a MEC service

High level requirements:

- UPF: Basic session attach
- UPF: May require support of inter-UPF communication (N9)
- UPF: Other functions can be highly tailored and simplified depending upon application
- All other functions provided by host service provider

Other considerations and potential requirements:

- LI functions of UPF likely not required (assumes that no interconnected services preclude LI)
- Charging/billing not required for MVC

Services required

- Termination of dedicated packet data connection for local breakout
- Basic connectivity – no need for DPI, firewall or other specialized services
- Others TBD

4. Open Core Application and Services Functional Requirements

The open core project consists of a set of services and applications that make up the essential elements of the wireless core network. These building blocks:

1. Shall include the network functions required for a minimally viable product (MVP) 5GC core: UPF, SMF, and AMF
   1.1. May optionally include other standard and non-standard network functions as required to meet project objectives
2. Shall be packaged flexibly allowing both "network in a box" deployment or selective deployment of project components
3. Shall be infrastructure agnostic
   3.1. Shall be agnostic to the operating environment (minimal to no ties to hardware environment or "undercloud", etc.)
   3.2. Shall not, to the extent reasonably possible, depend upon specific hardware selections or specialized equipment configurations
   3.3. Shall be designed for flexible deployment in a different operating environment, including a variety of public and private cloud environments, standalone deployments or integrated into other projects
4. Shall offer simple, templated onboarding with a bundled baseline schema
5. Shall be designed using a cloud native micro services architecture
6. Shall be managed using automation and orchestration tools developed as part of OCN
7. Can be deployed in a variety of configurations supporting differing user needs for reliability, scalability, and performance
8. Shall support rich tools for monitoring and visibility
9. Shall be deployable in a variety of configurations and capacities from very small (10s of UEs and 10Gbps throughput) to large scale (10m+ UEs and 400Gbps or higher throughput)
10. Shall include support for capabilities mandated by appropriate legal and regulatory agencies.

4.1. MVC Use-Case Specific Requirement Modifications

The first release of open core network will deliver a subset of the 5G-SA SBA network functions targeted to specific limited use cases as described in Chapter 4 if this document. the use cases described in chapter 3 have been evaluated as candidates to de-scope the development of a minimum viable core (MVC). For the MVC deployment the following use cases are considered in the following requirements:

1. Fixed Wireless Access
2. Private 5G
3. MEC

Other uses cases are out of scope for the MVC and will be considered in future versions of this specification. The following requirements are modified for each potential MVC use case. Requirements that apply to for each potential MVC use case are marked MVC. Mandatory requirements ("Shall" requirements) that are not marked may be considered out-of-scope for the MVC. Optional requirements that are marked MVC are considered mandatory that use case.

4.2. General Requirements

	Description
REQ-OCN-01	OCN shall deliver the network functions of the 3GPP 5G-SA core implemented using the SBA architecture
REQ-OCN-02	The initial release of OCN shall conform the 3GPP release 15.08
REQ-OCN-03	OCN may adopt later release of the 3GPP specification in future releases
REQ-OCN-04	OCN is to be developed in stages, starting with a 5G minimum viable core (MVC) and evolving to full 5G SBA core including support for multiple access methods as a converged core (3GPP opt 4)
REQ-OCN-05	OCN network functions shall provide 3GPP compliant implementations of the N1, N2, and N3 interfaces to the 5G radio access network
REQ-OCN-06	Each network function of OCN shall be able to stand alone and operate as an independent network function
REQ-OCN-07	Each network function of OCN shall be able to interoperate with network functions provided by other vendor's 5GC network functions using standard 3GPP reference point interfaces.

4.3. OCN Performance Requirements

Req #	Description
REQ-PERF-01	OCN network functions shall scale independently of each other
REQ-PERF-02	OCN network functions shall be horizontally scalable
REQ-PERF-03	OCN network functions may be vertically scalable (note: vertical scale may be increased by horizontal scaling of the microservices that make up the network function)
REQ-PERF-04	MVC: The OCN MVC shall support at least 1,000 UEs
REQ-PERF-05	MVC: The OCN MVC shall support at least 1,000 simultaneously attached PDC sessions
REQ-PERF-06	MVC: The OCN MVC shall support at least 10Gbps of bidirectional user data throughput

4.4. OCN Software Implementation

Req #	Description
REQ-SW-01	OCN shall deliver an open-source reference implementation of the OCN network functions
REQ-SW-02	OCN software components be constructed of microservices
REQ-SW-03	OCN software components be constructed to scale horizontally
REQ-SW-04	*deleted*
REQ-SW-05	*deleted*
REQ-SW-06	Software components of OCN shall be built to deploy on any platform that is compliant with the Cloud iNfrastructure Telco Taskforce (CNTT) specification
REQ-SW-07	OCN software components shall be designed to allow deployment on public cloud, private cloud, hybrid cloud or bare metal deployments
REQ-SW-08	OCN software components shall not depend on any cloud service provider proprietary services
REQ-SW-09	OCN software components may support IO acceleration technologies

REQ-SW-10	OCN software components of OCN shall shall comply with cloud-native design best practices as defined by CNTT
REQ-SW-11	OCN software components shall provide open metrics and monitoring capabilities
REQ-SW-12	OCN software components shall publish metrics on a standard exporter endpoint(s) compliant with CNTT specifications
REQ-SW-13	Software components of OCN may publish metrics by other APIs or methods (event streams, SNMP, etc.)

4.5. Network Function Requirements

4.5.1. User Plane Function (UPF) Requirements

Req #	Description	FWA	P5G	MEC
REQ-UPF-01	OCN shall include the UPF function	MVC	MVC	MVC
REQ-UPF-02	The OCN UPF shall expose the N4 interface as specified in 3GPP TS 29.244 (PFCP)	MVC	MVC	MVC
REQ-UPF-03	The OCN UPF may interface with other OCN software components using cloud native state exchange interfaces.	MVC	MVC	MVC
REQ-UPF-04	The OCN UPF shall implement the N3 interface as specified in 3GPP TS 29.281 (GTPv1-U)	MVC	MVC	MVC
REQ-UPF-05	The OCN UPF shall implement the N6 interface as specified in TS 29.281	MVC	MVC	MVC
REQ-UPF-06	The OCN UPF shall implement the N9 interface as specified in TS 29.274 (GTP v2)	MVC	MVC	MVC
REQ-UPF-07	The OCN UPF shall implement QoS enforcement			
REQ-UPF-08	The OCN UPF shall support mapping of IP QoS markings on N6 to/from PDU session QoS on N3			
REQ-UPF-09	The OCN UPF shall map radio link QoS (N3) to DN QoS (N6)			
REQ-UPF-10	The OCN UPF shall define methods inserting bearer flow services (e.g., DPI, NAT, etc.)			
REQ-UPF-11	The OCN UPF shall support IPv4 PDU types	MVC	MVC	MVC
REQ-UPF-12	The OCN UPF may support IPv6 PDU types			
REQ-UPF-13	The OCN UPF may support Ethernet PDU types			
REQ-UPF-14	The OCN UPF may support unstructured PDU types			
REQ-UPF-15	The OCN UPF shall support IPv4 transport on all interfaces	MVC	MVC	MVC

REQ-UPF-16	The OCN UPF may support IPv6 transport on any interface			
REQ-UPF-17	The OCN UPF may supply a network service header on the N6 interface compliant with IETF RFC 8300			
REQ-UPF-18	The OCN UPF shall support jumbo frames of at least 2,000 bytes MTU for bearer traffic on the N3, N6 & N9 interfaces			
REQ-UPF-19	The OCN UPF shall support LI/CALEA functions as specified in TS 133.138			
REQ-UPF-20	The UPF data path interfaces (N3, N6 & N9) shall support ARP requests for the IP address assigned to each interface			
REQ-UPF-21	The UPF data path interfaces (N3, N6 & N9) shall respond to ICMP ping requests			
REQ-UPF-22	The UPF data path interfaces (N3, N6 & N9) shall support fragmentation of IP packets transmitted based on the configured MTU of the interface			
REQ-UPF-23	The UPF data path interfaces (N3, N6 & N9) shall support IPv4 & IPv6 packet reassembly of packets received			
REQ-UPF-24	The OCN UPF shall provide mechanisms to support inline services such as CG-NAT, DPI, and others.			

4.5.2. Session Manager Function (SMF) Requirements

Req #	Description	FWA	P5G	MEC
REQ-SMF-01	The OCN shall include the SMF function	MVC	MVC	
REQ-SMF-02	The OCN SMF shall implement the N4 interface as specified in 3GPP TS 29.244 (PFCP)			
REQ-SMF-03	The OCN SMF may interface with other OCN software components using cloud native state exchange interfaces.	MVC	MVC	
REQ-SMF-04	The OCN SMF shall implement the Nsmf service interface as specified in TS 23.502			
REQ-SMF-05	<deleted>			
REQ-SMF-06	The OCN SMF shall support sessions with IPv4 PDU types	MVC	MVC	
REQ-SMF-07	The OCN SMF may support sessions with Ipv6 PDU types			
REQ-SMF-08	The OCN SMF may support sessions with Ethernet PDU types			
REQ-SMF-09	The OCN SMF may support sessions with Unstructured PDU types			
REQ-SMF-10	The OCN SMF may support Ipv4 transport on all interfaces			
REQ-SMF-11	The OCN SMF may support Ipv6 transport on any interface			
REQ-SMF-12	The OCN SMF shall support LI/CALEA functions as specified in TS 133.138			

4.5.3. Access and Mobility Function (AMF) Requirements

Req #	Description	FWA	P5G	MEC
REQ-AMF-01	OCN shall include the AMF function	MVC	MVC	
REQ-AMF-02	The OCN AMF shall implement the N1 interface as specified in TS 23.502	MVC	MVC	
REQ-AMF-03	The OCN AMF shall implement the N2 interface as specified in TS 23.502	MVC	MVC	
REQ-AMF-04	The OCN AMF shall implement the Namf service interface as specified in TS 23.502	MVC	MVC	
REQ-AMF-05	The OCN AMF may interface with other OCN software components using cloud native state exchange interfaces.	MVC	MVC	
REQ-AMF-06	For some MVC use cases, the OPN AMF may exclude procedures on N1	MVC		

	and N2 related to mobility and handoff			

4.5.4. Policy Control Function (PCF) Requirements

Req #	Description	FWA	P5G	MEC
REQ-PCF-01	OCN shall include the PCF function			
REQ-PCF-02	The OCN PCF shall implement the Npcf service interface as specified in TS 23.502			
REQ-PFC-03	The OCN AMF may use GRPC transport for the Npcf service interface			

4.5.5. Authentication Server Function (AUSF) Requirements

Req #	Description	FWA	P5G	MEC
REQ-AUSF-01	OCN shall include the AUSF function			
REQ-AUSF-02	The OCN PCF shall implement the Nausf service interface as specified in TS 23.502			
REQ-AUSF-03	The OCN AMF may use GRPC transport for the Nausf service interface			

4.5.6. User Data Manager Function (UDM) Requirements

Req #	Description	FWA	P5G	MEC
REQ-UDM-01	OCN shall include the UDM function			
REQ-UDM-02	The OCN PCF shall implement the Nudm service interface as specified in TS 23.502			
REQ-UDM-03	The OCN AMF may use GRPC transport for the Nudm service interface			

4.5.7. Network Resource Function (NRF) Requirements

Req #	Description	FWA	P5G	MEC
REQ-NRF-01	OCN shall include the NRF function			
REQ-NRF-02	The OCN PCF shall implement the Nnrf service interface as specified in TS 23.502			
REQ-NRF-03	The OCN AMF may use GRPC transport for the Nnrf service interface			

4.5.8. Network Exposure Function (NEF) Requirements

Req #	Description	FWA	P5G	MEC
REQ-NEF-01	OCN shall include the NEF function			
REQ-NEF-02	The OCN PCF shall implement the Nnef service interface as specified in TS 23.502			
REQ-NEF-03	The OCN AMF may use GRPC transport for the Nnef service interface			

4.5.9. Network Slice Selection Function (NSSF) Requirements

Req #	Description	FWA	P5G	MEC
REQ-NSSF-01	OCN shall include the NSSF function			
REQ-NSSF-02	The OCN PCF shall implement the Nnssf service interface as specified in TS 23.502			

REQ-NSSF-03	The OCN AMF may use GRPC transport for the Nnssf service interface			

4.5.10. Charging Function (CHF) Requirements

Req #	Description	FWA	P5G	MEC
REQ-CHF-01	OCN shall include the CHF function			
REQ-CHF-02	The OCN shall implement the Nchf service interface as specified in TS 32.291/32.255/32.290			
REQ-NSSF-03	The OCN CHF may use GRPC transport for the Nchf service interface			

4.6. Non-Functional Requirements

4.6.1. Availability

Req #	Description
REQ-Avail-01	OCN shall target service availability of 99.999%

4.6.2. Scalability

Req #	Description
REQ-Scale-01	OCN network functions shall support horizontal scaling (i.e., scaling by adding replicas)
REQ-Scale-02	Each OCN network function shall scale independently from other functions (i.e., no requirement to scale other NFs just because you scale another)

4.6.3. Upgrades and Restarts

Req #	Description
REQ-Restarts-01	OCN network functions shall be independently restartable without impact to other functions
REQ-Restarts-02	OCN network functions shall be upgradeable independently
REQ-Restarts-03	OCN interfaces shall be versioned allowing forward and backward compatibility
REQ-Restarts-04	OCN microservices shall make provision for canary upgrades

4.6.4. Deployment requirements and scenarios

Req #	Description
REQ-Deploy-01	TBD

5. GLOSSARY

3GPP The 3rd Generation Partnership Project (3GPP) is an umbrella for a number of standards organizations which develops protocols for mobile telecommunications. Its best-known work is the development and maintenance of GSM, UMTS, LTE, 5G, IP multimedia subsystem (IMS) and other related standards. 3GPP is a consortium with seven national or regional telecommunication standards organizations as primary members ("organizational partners") and a variety of other organizations as associate members ("market representation partners").

3G, 4G, 5G

The 3rd, 4th, and 5th generation cellular data technologies. 3G generally represents cellular data network that enabled the introduction of the smartphone and mobile web browsers; 4G represents true broadband internet access to mobile devices; 5G cellular technologies deliver massive bandwidth and reduced latency to cellular systems, supporting a range of devices from smartphones to autonomous vehicles and large-scale IoT. For completeness, 1G represented analog cellular voice systems and 2G represents early digital cellular voice system with limited data capabilities.

Access and Mobility Function (AMF)

A primary network function in the 3GPP 5G core. The AMF provides most of the control plan for the RAN, including NAS functions, UE authentication and security context, registration and connection management, reachability management, and mobility management. The AMF is also responsible to apply mobility related policies from PCF (e.g. mobility restrictions).

Access Network

A network that enables user devices access to network services. It is contrasted with the core network which connects service providers to one another.

Application Function (AF)

A primary Network Function in the 3GPP 5G Core.

Authentication Server Function (AUSF)

A primary network function in the 3GPP 5G core. The AUSF performs the UE authentication functions for the 5G network, including EAP authentication and the storage of network keys.

Base Station

A network function in the RAN which is responsible for the transmission and reception of radio signals in one or more cells to or from user equipment. A base station can have an integrated antenna or may be connected to an antenna array by feeder cables. Uses specialized digital signal processing and network function hardware. In modern RAN architectures, the base station may be split into multiple functional blocks operating in software for flexibility, cost and performance.

Centralized Data Center

A large, often hyperscale physical structure and logical entity which houses large compute, data storage and network resources which are typically used by many tenants concurrently due to their scale. Located a significant geographical distance from the majority of their users and often used for cloud computing.

Cloud Computing

A system to provide on-demand access to a shared pool of computing resources, including network, storage, and computation services. Typically utilizes a small number of large centralized data centers and regional data centers today.

Cloud Native Technologies

Cloud native technologies empower organizations to build and run scalable applications in modern, dynamic environments such as public, private, and hybrid clouds. Containers, service meshes, microservices, immutable infrastructure, and declarative APIs exemplify this approach. These techniques enable loosely coupled systems that are resilient, manageable, and observable. Combined with robust automation, they allow engineers to make high-impact changes frequently and predictably with minimal toil.

Cloud-native Network Function (CNF)

A virtualized network function (VNF) built and deployed using cloud native technologies. These technologies include containers, service meshes, microservices, immutable infrastructure and declarative APIs that allow deployment in public, private and hybrid cloud environments through loosely coupled and automated systems.

Cloud Service Provider (CSP)

An organization which operates typically large-scale cloud resources comprised of centralized and regional data centers. Most frequently used in the context of the public cloud. May also be referred to as a cloud service operator (CSO).

Core Network

The layer of the service provider network which connects the access network and the devices connected to it to other network operators and service providers, such that data can be transmitted to and from the internet or to and from other networks.

Jitter

The variation in network data transmission latency observed over a period of time. Typically measured in of milliseconds as a range from the lowest to highest observed latency values which are recorded over the measurement period.

Latency

The time taken by a unit of data (typically a frame or packet) to travel from its originating device to its intended destination. Typically measured in milliseconds. Latency generally refers to one-way delays between two devices. Round trip time (RTT).

Latency Critical Application

An application that will fail to function or will function destructively if latency exceeds certain thresholds. Latency critical applications are typically responsible for real-time tasks such as supporting an autonomous vehicle or controlling a machine-to-machine process. Unlike Latency Sensitive Applications, exceeding latency requirements will often result in application failure.

Latency Sensitive Application

An application in which reduced latency improves performance, but which can still function if latency is higher than desired. unlike a latency critical application, exceeding latency targets will typically not result in application failure, though may result in a diminished user experience. Examples include image processing and bulk data transfers.

Lawful Intercept (LI)

TBD

Local Breakout (LBO)

The capability to direct traffic to different endpoints, typically based on destination IP address, port and/or service. This permits traffic for edge services (MEC) to be processed locally while more general traffic can be routed to the service provider’s data centers or directly to the Internet.

Location-Based Node Selection

A method of selecting an optimal node on which to run a workload based on the node's physical location in relation to the device’s physical location with the aim of improving application workload performance. A part of workload orchestration.

Mobile Network operator (MNO)

The operator of a mobile network, who is typically responsible for the physical assets such as RAN equipment and network sites required for the network to be deployed and operate effectively. Distinct from MVNO as the MNO is responsible for physical network assets. May include those edge data centers deployed at the infrastructure edge positioned at or connected to their cell sites under these assets. Typically, also a service provider providing access to other networks and the internet.

Mobile Virtual Network operator (MVNO)

A service provider similar to an MNO with the distinction that the MVNO does not own or often operate their own cellular network infrastructure. Although they will not own an edge data center deployed at the infrastructure edge connected to a cell site they may be using, the MVNO may be a tenant within that edge data center.

Multi-Access Edge Computing (MEC)

An open application framework sponsored by ETSI to support the development of services tightly coupled with the radio access network (RAN). Formalized in 2014, MEC seeks to augment 4G and 5G wireless base stations with a standardized software platform, API and programming model for building and deploying applications at the edge of the wireless networks. MEC allows for the deployment of services such as radio-aware video optimization, which usescaching, buffering and real-time transcoding to reduce congestion of the cellular network and improve the user experience. Originally known as mobile edge computing, the ETSI working group renamed itself to multi-access edge computing in 2016 in order to acknowledge their ambition to expand MEC beyond cellular to include other access technologies. Uses edge data centers deployed at the infrastructure edge.

Network Exposure Function (NEF)

A primary Network Function in the 3GPP 5G core. The NEF provides a mechanism for securely exposing services and features of the 5G core.

- Exposes capabilities and events
- Secure provision of information from an external application to 3GPP network
- Translation of internal/external information
- Control plane parameter provisioning
- Packet flow description (PFD) management. A PFD is a tuple of protocol, server-side IP and port number.

Network Function

A functional building block within a network infrastructure which has a well-defined functional behaviour and well-defined interfacesA network function may be implemented as a physical entity (PNF) or software entities (VNF or CNF)

Network Function Virtualization (NFV)

The migration of network functions from physical network elements using embedded software running on proprietary hardware appliances to software based VNFs running on standard servers using industry standard virtualization and cloud computing technologies. In many cases NFV processing and data storage will occur at the edge data centers that are connected directly to the local cellular site, within the infrastructure edge.

Network Slice Selection Function (NSSF)

A primary network function in the 3GPP 5G core. The NSSF redirects traffic to a network slice. Network slices may be defined for different classes of subscribers. The NSSF performs the following functions:

- Selecting of the network slice instances to serve the UE
- Determining the allowed NSSAI
- Determining the AMF set to be used to serve the UE

Network Slicing

A network architecture that enables deploying independent logical networks on shared physical resources (network, storage, and compute).

Northbound vs Southbound (and east/west)

The direction in which data is transmitted when viewed in the context of a hierarchy where the cloud is at the top, the infrastructure edge is in the middle, and the device edge is at the bottom. Northbound and southbound data transmission is defined as flowing to and from the cloud or edge data center accordingly. Eastbound and westbound data transmission is defined as occurring between data centers at the same hierarchical layer, for purposes such as workload migration or data replication. This may occur between centralized or between edge data centers.

Open Core Network (OCN)

Telecom Infra Project (TIP) subgroup addressing applications and services, orchestration and automation issues.

Policy Control Function (PCF)

A primary network function in the 3GPP 5G core. The PCF provides:

- Policy rules for control plane functions, including network slicing, roaming and mobility management.
- Accesses subscription information for policy decisions taken by the UDR.
- Supports the new 5G QoS policy and charging control functions.

Quality of Experience (QoE)

The advanced use of QoS principles to perform more detailed and nuanced measurements of application and network performance with the goal of further improving the user experience of the application and network. Also refers to systems which will proactively measure performance and adjust configuration or load balancing as required. Can therefore be considered a component of workload orchestration, operating as a high-fidelity data source for an intelligent orchestrator.

Quality of Service (QoS)

A measure of how well the network and data center infrastructure is serving a particular application, often to a specific user. Throughput, latency and jitter are all key QoS measurement metrics which edge computing seeks to improve for many different types of application, from real-time to bulk data transfer use cases.

Radio Access Network (RAN)

A wireless variant of the access network, typically referring to a cellular network such as 3G, 4G or 5G. The 5G RAN will be supported by compute, data storage and network resources at the infrastructure edge as it utilizes NFV and C-RAN.

Round Trip Time (RTT)

The total latency for a unit of data to travel from one network endpoint and then

Service Based Architecture (SBA)

A software development paradigm which improves the modularity of products by breaking down them into interconnected microservices. The 3GPP defines a SBA as a set of Network Functions (NFs) that communicate with each other to provide/request services.

Service Provider

An organization which provides customers with access to its network, typically with the goal of providing that customer access to the internet. A customer will usually connect to the access network of the service provider from their side of the last mile.

Session Management Function (SMF)

A primary Network Function in the 3GPP 5G core. The SMF allocates IP addresses to UEs, handles NAS signalling for session management (SM), sends QoS and policy information to RAN via the AMF, provides downlink data notification. The SMF selects and controls the UPF for traffic routing. The SMF determines how the policy and charging for services is applied. The SMF is also responsible for lawful intercept on the control plane**.**

Throughput

In the context of network data transmission, the amount of data per second that is able to be transmitted between two or more endpoints. Measured in terms of bits per second typically at megabit or gigabit scales as required. Although a minimum level of throughput is often required for applications to function, after this latency typically becomes the application-limiting and user experience-damaging factor.

Traffic Offloading

The process of rerouting data that would normally be delivered inefficiently, such as over long distance, congested, or high cost networks, to an alternative, more local destination (e.g., a CDN cache) or on to a lower-cost or more efficient network. Local breakout is an example of using edge computing for traffic offloading.

Unified Data Management Function (UDM)

A primary network function in the 3GPP 5G core. The EDM provides user data management, including user identification, user access authorizations and subscription management.

User Plane Function (UPF)

A primary network function in the 3GPP 5G Core. The UPF provides the mobility anchor for 5G user data plane allowing handoff between various nodes in the radio access network. The UPF may also implement inspection and classification functions such as NAT, firewall, application detection and other services. The UPF is also responsible usage tracking and reporting for charging and user plan lawful intercept.

Virtualized Network Function (VNF)

A software-based network function operating on general-purpose compute resources which is used by NFV in place of dedicated physical equipment. In many cases, several VNFs will operate on an edge data center at the infrastructure edge.