वर्गीय आवश्यकताओं के लिए मानक

टी.ई.सी २१११२०:२०२४

STANDARD FOR GENERIC REQUIREMENTS

TEC 21120:2024

छोटे आकार का 5जी कोर

Small Size 5G Core

ISO 9001:2015

दूरसंचार अभियांत्रिकी केंद्र

खुर्शीदलाल भवन, जनपथ, नई दिल्ली-११०००१, भारत

TELECOMMUNICATION ENGINEERING CENTRE

KHURSHIDLAL BHAWAN, JANPATH, NEW DELHI–110001, INDIA

www.tec.gov.in

Release1: November, 2024

FOREWORD

Telecommunication Engineering Centre (TEC) functions under Department of Telecommunications (DOT), Government of India. Its activities include:

- Issue of Standards for Generic Requirements (GR), Interface Requirements (IR) and Service Requirements (SR) as well as Test guides for Telecom Products and Services;
- Issue of Technical regulations in the form of essential Requirements (ER);
- Field evaluation of products and Systems;
- National Fundamental Plans;
- Support to DOT on technology issues;
- Testing & Certification of Telecom products; and
- Designation of Conformance Assessment Bodies (CABs) for testing.

For the purpose of testing, four Regional Telecom Engineering Centers (RTECs) have been established which are located at New Delhi, Bangalore, Mumbai, and Kolkata.

ABSTRACT

This document is the standard for the Generic Requirements (GR) of "Small Size 5G Core" based mobile system which is a compact, cost effective, power efficient 5G SA (Stand-alone) Core targeted for Private Networks, Temporary 5G Connectivity Requirements for Special Purposes, Disaster Management etc. for deployment in the Indian mobile communication network.

The document covers the functional requirements, general requirements and features of the system including OMC/EMC Requirements.

CONVENTIONS

In this document, requirements are classified as follows:

- The keywords "shall" or “is/are required to” indicate a requirement or requirements, which must be mandatorily complied and from which no deviation is permitted, if conformance to this document is to be claimed; and

- The keywords “optional” or “may” indicate an optional requirement, which is permissible for exclusion from mandatory compliance, unless the said requirement is claimed to be complied by the vendor. These terms are not intended to imply that the vendor's implementation must provide the option; it means the vendor may optionally provide the feature and still claim conformance with this document.

CONTENTS

Clause * Particulars ***Page No.***

HISTORY SHEET

S.No.	*GR No.*	*Title*	*Remarks*
1.	TEC 21120:2024	Standard for Generic Requirement of Small Size 5G Core	Release 1

REFERENCES

S. No.	TEC Standard No./3GPP/ Intl Standard/Government Order	Title/Document Name
1.	3GPP TS 23.501	5G; System architecture for the 5G System (5GS)
2.	3GPP TS 23.502	5G; Procedures for the 5G System (5GS)
3.	3GPP TS 33.501	5G; Security architecture and procedures for 5G System
4.	3GPP TS 29.502	5G; 5G System; Session Management Services; Stage 3
5.	3GPP TS 32.255	5G; Telecommunication management; Charging management; 5G data connectivity domain charging; Stage 2
6.	3GPP TS 23.503	5G; Policy and charging control framework for the 5G System (5GS); Stage 2
7.	3GPP TS 29.244	LTE; 5G; Interface between the Control Plane and the User Plane nodes
8.	3GPP TS 23.632	LTE; 5G; User data interworking, coexistence and migration; Stage 2
9.	3GPP TS 29.510	5G; 5G System; Network function repository services; Stage 3
10.	3GPP TS 29.513	5G; 5G System; Policy and Charging Control signalling flows and QoS parameter mapping; Stage 3
11.	3GPP TS 29.521	5G; 5G System; Binding Support Management Service; Stage 3
12.	3GPP TS 32.290	5G; Telecommunication management; Charging management; 5G system; Services, operations and procedures of charging using Service Based Interface

		(SBI)
13.	3GPP TS 29.504	5G; 5G System; Unified Data Repository Services; Stage 3
14.	3GPP TS 29.520	5G; 5G System; Network Data Analytics Services; Stage 3
15.	3GPP TS 32.240	LTE; Telecommunication management; Charging management; Charging architecture and principles
16.	3GPP TS 23.041	Digital cellular telecommunications system (Phase 2+) (GSM); Universal Mobile Telecommunications System (UMTS); LTE; 5G; Technical realization of Cell Broadcast Service (CBS)

CHAPTER 1

1 Introduction

1.1 Overview

This document contains standard for the Generic Requirements (GR) of “Small Size 5G Core” based mobile system which is a compact, cost effective, power efficient 5G SA (Stand-alone) Core targeted for Private Networks, Temporary 5G Connectivity Requirements for Special Purposes, Disaster Management etc. for deployment in the Indian mobile communication network.

The document covers the functional requirements, general requirements and features of the system. including OMC/EMC Requirements.

1.2 Objective

The key objective of Small Size 5G Core is to have a compact, cost effective, power efficient which addresses the requirements in terms of coverage, capacity and quality with ease of deployment and ease of maintenance.

1.3 Applications

As the system is small, compact 5G core, it may be suitable for providing the 5G mobile communication services, for the following applications as required:

i. Private Networks: In this application, the system may be either used in isolation/ stand-alone mode or may have connectivity with public/ private mobile communication network with/without roaming support.
ii. Temporary 5G Connectivity Requirements for Special Purposes: The system may be used to provide temporary 5G mobile connectivity at special events such as sporting events, conventions, short term projects and fairs, scientific exploration camps in uncovered areas, etc. for limited number of

users. It may or may not have connectivity with public/ private mobile communication network with/without roaming support.

iii. Disaster Management: In this application, the system, being compact and power efficient, may be used to provide easy and quick deployment for providing 5G mobile communication facility in time of emergency during disaster. The system may operate on non-conventional energy sources in the absence of commercial electric supply as a standalone communication system. In this scenario, the system may have connectivity with public/ private mobile communication network with or without roaming support.

1.1 Deployment Methodology

It is worthwhile to distinguish what small means in in terms of capacity and deployment for the 5G core. Some example deployments are given below.

i. For a private network, like in a factory, there data throughput requirements are likely to be larger due to the presence of lot of audio-visual devices as well as large number of sensors emitting data across the factory. In this case, it should be prudent to have a hybrid deployment where some time sensitive applications are deployed locally in the factory and other generic applications being deployed in the cloud network. This means that dedicated dataplane (UPF) is deployed on premise for time sensitive applications whereas cloud based UPFs cater to the generic applications.

ii. For temporary deployments, since catering to security personnel or event management personnel would be priority, a small footprint core could be deployed. However, since the temporary deployments can be planned, the core can be deployed in cloud.

iii. For a disaster zone, if the only priority is to connect the rescue workers, the overall throughput requirements are likely to be small. Also, the network would need to be quickly deployable with minimum infrastructure requirements. So, a possible solution example could be a 5G core deployed in

a one or two VMs or as a containerised solution that can fit in a drone or backpack having minimal footprint.

CHAPTER 2

2 Small sized 5G Core

The Small sized 5G Core Network utilizes service-based architecture (SBA) that spans across 5G functions and provides authentication, security, session management, mobility management connectivity and data access.

The Network Functions (NFs) of the 5G Core Network are:

i). Access and Mobility management Function (AMF);

ii). Session Management Function (SMF);

iii). User Plane Function (UPF).

iv). Authentication Server Function (AuSF);

v). Unified Data Management (UDM);

vi). Unified Data Repository (UDR);

vii). Network Repository Function (NRF);

viii). Policy Control Function (PCF);

ix). Network Exposure Function (NEF);

x). Network Slice Selection Function (NSSF);

xi). Binding Support Function (BSF);

xii). Charging Function (CHF);

xiii). Short Message Service Function (SMSF)

xiv). Network Data Analytics Function (NWDAF)

xv). Security Edge Protection Proxy (SEPP)

xvi). Service Communication Proxy (SCP)

xvii). Non-3GPP Interworking Function (N3IWF)

xviii). LMF (Location Management Function)

xix). CBCF (Cell Broadcast Control Function)

In addition, Operation and Management (OAM) System may also form part of 5G Mobile Network. Further, IP Multimedia Subsystem (IMS) may be required in case

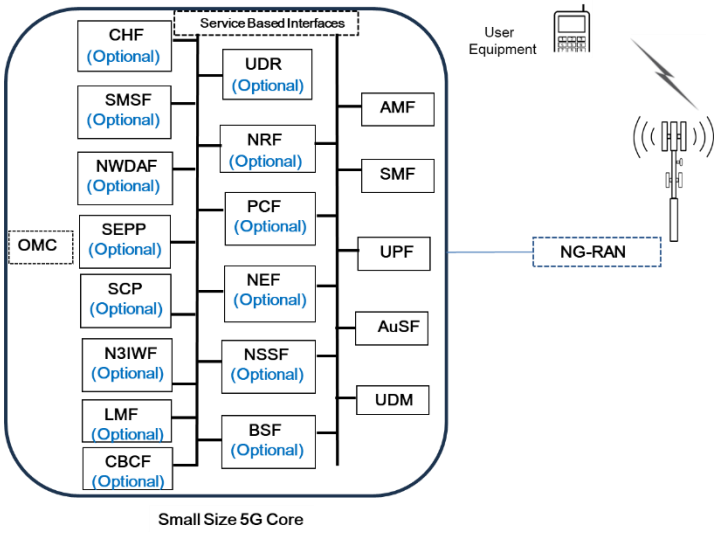
of specific deployments. Similarly, MCX functionality may be required in case of specific deployments.

NOTE 1: In the case of Small Sized 5G Core, some of the NFs viz. BSF, CHF, NRF, NEF, NSSF etc. may or may not be required, depending on specific deployment. As such, all the above-mentioned NFs may not be required to be implemented.

NOTE 2: The procurer is required to specify the NFs, which are needed based on their deployment scenario.

NOTE 3: The manufacturer(s)/ vendor(s) are required to specify the NFs implemented in their system, while offering for testing/ certification for type approval/ technology approval/ certificate of approval.

A representative architecture of the small size 5G Core with the constituent Network Functions is shown below.



2.1 Interfaces for small sized 5G Core network:

This section describes an exhaustive list of 5G System service-based interfaces. The applicability of interfaces is enumerated in specific sections related to NFs.

2.1.1 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.

Nnsacf: Service-based interface exhibited by NSACF

Nnssaaf: Service-based interface exhibited by NSSAAF.

Nnssf: Service-based interface exhibited by NSSF.

NAuSF: Service-based interface exhibited by AuSF.

Nudr: Service-based interface exhibited by UDR.

Nudsf: Service-based interface exhibited by UDSF.

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

Nnwdaf: Service-based interface exhibited by NWDAF.

Nchf: Service-based interface exhibited by CHF.

Nucmf: Service-based interface exhibited by UCMF.

Ndccf: Service based interface exhibited by DCCF.

Nmfaf: Service based interface exhibited by MFAF.

Nadrf: Service based interface exhibited by ADRF.

Naanf: Service-based interface exhibited by AANF.

N5g-ddnmf: Service-based interface exhibited by 5G DDNMF.

Nmbsmf: Service-based interface exhibited by MB-SMF.

Nmbsf: Service-based interface exhibited by MBSF.

Ntsctsf: Service-based interface exhibited by TSCTSF.

Nbsp: Service-based interface exhibited by an SBI capable Bootstrapping Server Function in GBA.

Neasdf: Service-based interface exhibited by EASDF.

Nlmf Service-based interface exhibited by LMF

NOTE: In the case of Small Size 5G Core, some of the Service-based interfaces viz. Nnsacf, Nnssaaf, Nudsf, N5g-eir, Nnwdaf, Nchf, Nucmf, Ndccf, Nmfaf, Nadrf, Naanf, N5g-ddnmf, Nmbsmf, Nmbsf, Ntsctsf, Nbsp, Nlmfand Neasdf may or may not be required.

2.1.2 Reference Points

This section describes an exhaustive list of 5G System architecture reference points. The applicability of reference points is enumerated in specific sections related to NFs.

The 5G System Architecture contains the following reference points:

N1: Reference point between the UE and the AMF.

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

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

N4: Reference point between the SMF and the UPF.

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

N9: Reference point between two UPFs.

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

N5: Reference point between the PCF and an AF or TSN AF.

N7: Reference point between the SMF and the PCF.

N8: Reference point between the UDM and the AMF.

N10: Reference point between the UDM and the SMF.

N11: Reference point between the AMF and the SMF.

N12: Reference point between AMF and AuSF.

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

N14: Reference point between two AMFs.

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

N16a: Reference point between SMF and I-SMF.

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

N18: Reference point between any NF and UDSF.

N19: Reference point between two PSA UPFs for 5G LAN-type service.

N22: Reference point between AMF and NSSF.

N23: Reference point between PCF and NWDAF.

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

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

N28: Reference point between PCF and CHF.

N29: Reference point between NEF and SMF.

N30: Reference point between PCF and NEF.

NOTE 1:The functionality of N28 and N29 and N30 reference points are defined in 3GPP TS 23.503 (TEC Standard No. 25981:2022)

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

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

N32: Reference point between a SEPP in one PLMN or SNPN and a SEPP in another PLMN or SNPN; or between a SEPP in a SNPN and a SEPP in a CH/DCS, where the CH/DCS contains a UDM/AuSF.

NOTE 3: The functionality of N32 reference point is defined in 3GPP TS 33.501.

N33: Reference point between NEF and AF.

N34: Reference point between NSSF and NWDAF.

N35: Reference point between UDM and UDR.

N36: Reference point between PCF and UDR.

N37: Reference point between NEF and UDR.

N38: Reference point between I-SMFs and between V-SMFs.

N40: Reference point between SMF and the CHF.

N41: Reference point between AMF and CHF in HPLMN.

N42: Reference point between AMF and CHF in VPLMN.

NOTE 4:The functionality of N40, N41 and N42 reference points are defined in 3GPP TS 32.240.

N43: Reference point between PCFs.

NOTE 5:The functionality of N43 reference point is defined in TS 23.503 (TEC Standard No. 25981:2022)

NOTE 6: The reference points from N44 up to and including N49 are reserved for allocation and definition in 3GPP TS 32.240.

N50: Reference point between AMF and the CBCF.

N51: Reference point between AMF and NEF.

N52: Reference point between NEF and UDM.

N55: Reference point between AMF and the UCMF.

N56: Reference point between NEF and the UCMF.

N57: Reference point between AF and the UCMF.

NOTE 7: The Public Warning System functionality of N50 reference point is defined in 3GPP TS 23.041.

N58: Reference point between AMF and the NSSAAF.

N59: Reference point between UDM and the NSSAAF.

N60: Reference point between AuSF and NSWOF.

NOTE 8: The functionality of N60 reference point is defined in 3GPP TS 33.501.

N80: Reference point between AMF and NSACF.

N81: Reference point between SMF and NSACF.

N82: Reference point between NSACF and NEF.

N83: Reference point between AuSF and NSSAAF.

N84: Reference point between TSCTSF and PCF.

N85: Reference point between TSCTSF and NEF.

N86: Reference point between TSCTSF and AF.

N87: Reference point between TSCTSF and UDM.

N88: Reference point between SMF and EASDF.

NOTE 9:The reference points from N90 up to and including N95 are reserved for allocation and definition in 3GPP TS 23.503 (TEC Standard No. 25981:2022)

NOTE: In the case of Small Size 5G Core, some of the Service-based interfaces viz. Nnsacf, Nnssaaf, Nudsf, N5g-eir, Nnwdaf, Nchf, Nucmf, Ndccf, Nmfaf, Nadrf, Naanf, N5g-ddnmf, Nmbsmf, Nmbsf, Ntsctsf, Nbsp and Neasdf may be optional, as such, the corresponding reference points will also be optional in line with those interfaces.

CHAPTER 3

3 Network Functions

3.1 AMF (Access and Mobility Management)

AMF accesses the UE and the Radio Access Network in the signalling (control) plane

3.1.1 AMF Functional Requirements

a. The AMF shall be capable of connecting to:

i). AuSF;

ii). NG-RAN;

iii). SMF; and

iv). UDM.

b. The AMF Shall Support:

i). Primary authentication with AuSF using SUCI or SUPI for 5G AKA with SBI.

ii). At least one 3GPP based option of Control Plane signalling confidentiality and integrity protection of NAS signalling.

iii). UE initiated PDU session release procedure in connected state.

iv). UE triggered service request procedure and response with a service accept/reject message.

c. The AMF may support:

i). Network initiated PDU session release procedure when the UE is in idle state.

ii). Rejecting PDU session establishment based on SUPI and DNN

iii). The AMF may provide the SMF with the PEI (Permanent EquipmentIdentifier) of the UE if the PEI is available with the AMF at the time of PDU session establishment.

iv). one CBCF or multiple CBCFsto provide PWS.

v). Location services for transport for Location Services messages between UE and LMF as well as between RAN and LMF, in case of deployed disaster or temporary networks.

vi). Roaming –Communication with the H-AUSF and H-UDM for authentication (N12 interface) and obtaining subscription information (N8 interface).

vii). The AMF may be capable of connecting to:

a) PCF

3.2 SMF (Session Mangement Function)

SMF handles the calls and sessions, and contacts the UPF accordingly.

3.2.1 SMF functional requirements:

a. The SMF shall be capable of connecting to the

i). AMF;

ii). UPF;

iii) UDM;

b. The SMF may be capable of connecting to

(i) CHF.

(ii) PCF

c. The SMF shall support:

i). Session establishment between UPF and NG-RAN node.

ii). Selection and control of UPF function.

iii). Deletion of the UE PDU session when it receives the request

1. The cause IE set to “REL_DUE_TO_DUPLICATE_SESSION_ID” from AMF;
2. The cause IE set to “REL_DUE_TO_SLICE_NOT_AVAILABLE” from AMF[1] (Optional).

iv). Allocation of IPv4 address and/or Ipv6 prefix based on subscription information received from UDM.

d. The SMF may support:

i). UE IP address allocation and management.

ii). Local UPF within a PDU session.

iii). Converged online and offline charging

iv). Charging of PDU session using SBI interface

v). CHF selection based on the Charging Characteristics or using NRF[2]

vi). Sending of Charging Data Request [Termination] when abort request is received from the CHF

vii). Sending of Charging Data Request [update] and start new counts with time stamps at the start of new QoS flows which is not associated with default QoS rule.

viii). Sending of Charging Data Request [Update] and close the count with time stamp on expiry of time limit per PDU session.

[1] To be supported if network slicing feature is needed as per requirement of procurer.
[2] NRF part applicable, when NRF is part of the deployment.

ix). Sending of Charging Data Request [Update] and close the count with time stamp on expiry of data volume limit per PDU session.

x). Not informing the AMF of DL Data notification if the SMF is aware that the UE is unreachable or if the UE is reachable only for prioritized services which does not include PDU session.

xi). Roaming – Communication with H-SMF over N16 interface for PDU session establishment. [Note that the H-SMF interacts with the H-PCF for obtaining SM Policy and not the V-SMF]

3.2.2 SMF QoS requirements:

a. The SMF shall support:

i). QOS and Policy management support .Default QoS flows

ii). Dedicated QoS flows [3]

iii). 5QI values for eMBB

iv). Minimum 1 QOS flow per UE. Upto 16 QoS flows per UE is optional

v). Inclusion of GFBR and MFBR in QOS Profile for each GBR QoS Flow.

b. The SMF may support

i). QoS handling on Flow level, Service level as well as Session level.

ii). Both pre-configured and/or dynamically assigned 5QI.

iii). Operator-specific 5QI in the range of 128-254.

iv). QCI 65, 66, 69 and 70 - In case of support for MCX services

v). Appropriate QCI values for URLLC use cases, depending on procurer requirement based on deployment scenario

[3] To be supported in case VoNR is implemented.

vi). Appropriate QCI values for mMTC use cases, depending on procurer requirement based on deployment scenario

vii). Packet marking for HTTP/2 signaling over SBI.

NOTE: IP address, IMSI & Location may be logged for security purpose.

3.3 UPF (User Plane Function)

UPF represents the data plane evolution of a Control and User Plane Separation (CUPS) strategy, which is a fundamental component of the 3GPP 5G Core network.

3.3.1 UPF Functional Requirements

a. The UPF shall be capable of connecting to the:

   i). SMF;

   ii). NG-RAN;

   iii). Data Network; and

b. The UPF shall support:

   i). Packet Detection based on predefined PDRs or PDRs received in the PFCP messages from the SMF over N4 interface.

   ii). A PDU session that carries Ipv4 traffic.

   iii). QoS Flow ID (QFI) used to identify a QoS flow.

   iv). User Plane Traffic to QoS flows based on the SDF templates.

c. The UPF may support:

   i). Buffering of packets instead of immediately forwarding them based on the instructions received from the control plane.

   ii). Downlink Data Notification functionality.

iii). Monitoring the amount of downlink traffic that is dropped and report when a threshold is received as per the URR (Usage Reporting Rules) received from the SMF.

iv). User Traffic Redirection based on Destination IP

v). A PDU session that carries Ipv6 traffic.

vi). Application detection.

vii). Normalization of host server names in non-standard URLs in HTTP POST request messages so that HTTP post requests can be classified as standard requests.

viii). Tethering detection based on TTL values.

ix). Multi-homed PDU session.

x). HTTP Pipelining Request-Response matching enabling the user plane to match each HTTP response with the corresponding HTTP request.

xi). Service chaining functionality allowing the user plane to steer subscriber traffic to third-party service functions in the N6 or Sgi-LAN.

xii). Sending User Plane Inactivity Report to the SMF as a response when instructed.

xiii). N4 session level report procedure based on Usage Report;

xiv). N4 session level report procedure:

1. Start of traffic detection;
2. Stop of traffic detection; and
3. Detection of PDU session inactivity for a specified period.

xv). Roaming- Communication between visited UPF and Home UPF using the N9 interface.

xvi).

3.3.2 UPF QoS requirements:

a. The UPF shall support:

i). Non-guaranteed flow bit rate QoS flows.

ii). Enforcement of PDU session AMBR across all non-GBR QoS flows of a PDU session.

iii). Dropping packets if any packet exceeds the limits of any of the associated QERs.

b. The UPF may support

i). The QOS Flow for Guaranteed flow bit rate QoS flows;

ii). Transport level packet marking with a DSCP value.

iii). Inclusion of QFI and an indication for reflective QoS activation in the encapsulation header.

iv). The Reflective QoS Indication (RQI) in the encapsulation header on N3 reference point together with the QFI.

v). Marking of PDU session containers over the N3 interfaces with a QFI value that the control plane provides in a QER (QoS Enforcement Rule).

3.4 UDM (Unified Data Management)

UDM is a centralized way to control network user data.

3.4.1 UDM functional requirements:

a. UDM shall be connected with other 3GPP network elements using standard Interfaces:

   i). SMF, N10;

   ii). AMF, N8;

   iii). AUSF, N13;

b. UDM may be connected with other 3GPP network elements using standard Interfaces:

   i). SMSF, N21.

   ii). UDR, N35;

c. The UDM shall support:

   i). Following high level features:

      1. Identification and authentication;

   ii). Maintenance of AMF/SMF registration session.

   iii). Sending of deregistration notification using Nudm_UECM_DeregistrationNotification to NF consumer.

   iv). Data retrieval operation based on different query parameters (PLMN, NSSAI, DNN) and accordingly maintain session of subscriber.

   v). UE Authentication to provide updated authentication related subscriber data to the subscribed NF consumer.

   vi). Subscription of AMF and notify the AMF when subscription data is changed.

vii). Network-initiated deregistration requested by AMF using Nudm_UECM_DeregistrationNotification operation. Following Authentication related features:

1. Generation of 3GPP AKA Authentication Credentials;
2. Selection of the 5G-AKA authentication method so that network Function Service Consumer (e.g. AMF) returns the result received from the UE to the AUSF;
3. Different protection scheme;
4. Support of de-concealment of privacy-protected subscription identifier (SUCI);

viii). Following NRF services:

1. Nnrf_NFDiscovery service;
2. NFRegister, NFUpdate, NFDeregister service;
3. NF Heart-Beat service;
4. Deletion of stale security context; And
5. Use of NF discovery service on expiry of validity Period.

d. The UDM may support:

i). Services (Get/Subscribe/ Unsubscribe/ Update) via the Nudm interface for subscriber data Management.

ii). The EAP-based authentication method;

iii). UDM data replication across multiple small size 5G Core network, which will enable UE to move from one small sized 5G Core network to another;

iv). Following high level features:

1. Network slice selection;
2. Access control and barring; and
3. Lawful Interception

v). Generation and storage of keys using HSM to protect long-term keys from physical attacks and to keep them in the secure environment.

vi). Interworking with HSS:

1. UDM shall provide support to Service based interfaces for direct UDM-HSS interworking;
2. Terminating-Access Domain Selection for 5G access via UDM-HSS interworking; and
3. P-CSCF restoration via UDM-HSS interworking.

vii). Following Authentication related features:

1. Support of MT-SMS delivery support services; and
2. MT-SMS delivery support for short Message Roaming Routing, Set Message Waiting Data, Report SM-Delivery Status.

viii). Following NRF services:[4] (Optional)

1. NFStatusSubscribe, NFStatusNotify, NFStatusUnSubscribe service;
2. NFListRetrieval service;
3. NFProfileRetrieval service;
4. Nnrf_AccessToken service; and
5. Validation of expire time present in token validation response from NRF.

3.5 AuSF (Authentication Server Function)

AuSF is responsible for the security procedure for SIM authentication using the 5G-AKA authentication method.

3.5.1 AuSF functional requirements:

a. AuSF shall be connected with other 3GPP network elements using standard interfaces.

i). UDM, N13; and

[4] NRF services may be applicable depending on procurer requirement based on deployment scenario.

ii). AMF, N12.

b. The AuSF shall support:

i). At least one from Null, Profile-A or Profile-B.

ii). UE authentication service to the requester NF using Nausf_UEAuthentication.

iii). Setting of the authResult to AUTHENTICATION FAILURE, if the UE is not authenticated.

iv). 5G-AKA procedures.

v). UE id (e.g. SUPI or SUCI), Serving Network Name in the “authenticate” service request by NF.

vi). Provision of 4xx/5xx http status codes with message containing a Problem details structure with "cause" attribute set to one of the application error on failure in 5G-AKA and/ or 5G-EAP-AKA procedure (5G-EAP-AKA procedure, if supported).

vii). Following NRF services (if NRF is present):

1. Nnrf_NFDiscovery service;
2. NFRegister, NFUpdate and NFDeregister service;
3. NF Heart-Beat service;
4. NFStatusSubscribe service and NFStatusNotify service

c. The AuSF may support:

i). 5G-EAP-AKA procedures;

ii). Sending of NF access token request towards NRF after expiry of previous token:

1. AUSF shall use NF discovery service on expiry of validity Period; and
2. AUSF shall validate expire time present in token validation response from NRF.

iii). Both On-demand as well as Periodic/Scheduled backup procedures; (backup manual from the OMC/EMS)

3.6 UDR (Unified Data Repository)

UDR enables network functions to store and access subscription information.

NOTE: In the case of Small Size 5G Core, UDR services may be applicable depending on procurer requirement based on deployment scenario.

3.6.1 UDR functional requirements:

a. UDR shall be connected with other 3GPP network elements using standard service-based interface:
   i). UDM, N35;
   ii). PCF, N25; and
   iii). NEF, N37.

b. The UDR shall support:
   i). Authorization of user equipment.
   ii). Storage of access and mobility data and session management data needed by NF consumers to implement application logic.
   iii). Deletion of existing user data when a provisioning front end deletes a service profile for an existing user or profile for which consumer propose to remove an application data record.
   iv). Storage of new user data from NF service consumer, e.g., when a provisioning Front end consumer creates a profile for a new user or creates a new service profile for an existing user, or NF service consumer intends to insert a new application data record into the UDR.
   v). Authorization management mechanism to guarantee the safety of data access also access control in terms of read/write and level of service data to be accessed.
   vi). User confidentiality protection functionalities:
      1. Providing globally unique 5G Subscription Permanent Identifier (SUPI) to each subscriber in the 5G System and provisioned in the UDM/UDR;
      2. Supporting Permanent Equipment Identifier (PEI) to assume different formats for different UE types and use cases;

3. And HTTP GET and HTTP POST method for Query and subscribe operation; and
4. Ability to identify and remove inconsistent data.

c. The UDR may support:

i). Nudr_DataRepository services - Service operations like Create, Delete, Update, Notify, Subscribe, unsubscribe;

ii). User confidentiality protection functionalities:

1. Monitoring of various events configured via UDM

iii). Load Balancing Functionalities:

1. Supporting overload protections within UDR architecture and implementation to prevent processing overload of the UDR from application layer;
2. Providing redundancy models for each load balancing; and
3. An overload threshold value shall be set. Once the UDR loading reaches the threshold value, the system shall generate alarms before service impact.

iv). Different Redundancy mechanism procedures:

1. The UDR system redundancy shall support several levels of redundancy like data redundancy, site level redundancy, Network redundancy;
2. UDR shall support High-Availability to guarantee carrier-grade 99.999% system availability and avoid any Single Point of Failure; and
3. UDR shall implement geographical redundancy in order to support a disaster recovery configuration which guarantees no impact on services in case of a complete outage of a site as well.

v). 1+1 or 1+1+1 redundancy at data service level.

vi). Following NRF services:[5] (Optional)

1. NFStatusSubscribe, NFStatusUnsubscribe, NFRegister;

[5] NRF services may be applicable depending on procurer requirement based on deployment scenario

2. NFUpdate, NFDeregister, NFListRetrieval, NFProfileRetrieval;
3. Nnrf_AccessToken service, Heat Beat Service mechanism;
4. Nnrf_NFManagement service; and
5. Nnrf_NFDiscovery service.

3.7 NRF (Network Repository Function)

NRF controls, the other Network Functions (NFs) by providing support for NF register, deregister and update service to NF and their services.

NOTE: In the case of Small Size 5G Core, NRF services may be applicable depending on procurer requirement based on deployment scenario.

3.7.1 NRF functional requirements:

a. NRF shall be connected with other 3GPP network elements using standard Service Based Interface (SBI)
   i). AMF;
   ii). SMF
   iii). UDM;
   iv). AUSF;
   v). NEF;
   vi). PCF; and
   vii). NSSF.
b. NRF may be connected with other 3GPP network elements using standard Service Based Interface (SBI)
   i). SMSF;
   ii). UPF.
c. The NRF shall support:
   i). Following services:
      1. Nnrf_NFManagement service;
      2. Nnrf_NFDiscovery service;
      3. NFRegister service;
      4. NFUpdate service;

5. NF Heart-Beat service;
6. NFDeregister service;
7. NFStatusSubscribe service;
8. NFStatusNotify service;
9. NFStatusUnSubscribe service;

ii). Subscription and notification to other NFs regarding the registration in NRF of new NF instances of a given type.

iii). Subscription of NF to be notified of registration, deregistration and profile changes of NF Instances, along with their potential NF services.

iv). Nnrf_NFManagement service to allow NF to retrieve a list of NF and SCP Instances currently registered in the NRF or the NF Profile of a given NF Instance.

v). NF Register Service. It allows an NF or SCP Instance to register its profile in the NRF; it includes the registration of the general parameters of the NF Instance, together with the list of potential services exposed by the NF Instance.

vi). Support for NFDeregister Service request.

d. NRF may support:

i). Following services:

1. Nnrf_AccessToken service;
2. Nnrf_Bootstrapping service
3. NFListRetrieval service; and
4. NFProfileRetrieval service.

ii). Deployment on shared-slice level (the NRF is configured with information belonging to a set of Network Slices).

iii). Data structures and URI query parameters as defined in 3GPP TS 29.510 Clause 6.1.3.2.3.1.

iv). Ability to send requests to SEPP in weighted or priority mode or combination of these.

v). Blocking of Register operation to be invoked from an NRF in a different PLMN.

vi). Configuration with multiple PLMN IDs and registering, updating and deregistering the profile of Network Function Instances from any of these PLMN IDs.

vii). Changing the NFStatus of a NF to SUSPENDED if the NRF detects that the NF is no longer operative using the NF Heart-Beat procedure or by update procedure if the NF is still operative as per 3GPP TS 29.510 Section 5.2.2.3.2.

viii). Forwarding subscription request on basis of (target) PLMN-ID & NF-type if pre-configured routing policy is present. Precedence shall be given to routing Policy.

ix). Sending of POST request directly from NRF-2 to the NF Service Consumer without involvement of NRF-1 for Notification for subscription via Intermediate NRF.

x). Forwarding request to locally configured/registered forwarding NRF of same PLMN, in case of multiple NRF scenario. NRF2 shall send “307 temporary redirect” response to NRF1 containing location header of service producer NRF (If available locally otherwise 404). NRF1 shall re-initiate request to NRF3 and shall forward response towards requester NF as per 3GPP TS 29.510 Section 5.4.2.2.3.

xi). Generic data of each NF Instance, applicable to any NF type, and it may also contain NF-specific data, for those NF Instances belonging to a specific type (e.g., the attribute “udrInfo” is typically present in the NF Profile when the type of the NF Instance takes the value “UDR”) in NF Profile object returned in successful discovery response. In addition, the attribute “customInfo”, may be present in the NF Profile for those NF Instances with custom NF types as per 3GPP TS 29.510 Section 5.3.2.2.2.

xii). Multiple level of recovery from software and hardware faults such that the impact on system operation shall be in accordance to the severity of the faults. In other words, not all software or hardware faults shall cause system or application recovery that has system wide impact.

xiii). Establishment of connection with Secondary SEPP IP for forwarding the same request, in case when request timeout is received from Primary SEPP IP.

xiv). Geo-redundancy and disaster recovery architecture without any data loss or service outage.

xv). Roaming - Communication with H-NRF to resolve the home PLMN network functions over N27 interface via SEPP.

3.8 PCF (Policy Control Function)

PCF controls that the user data traffic does not exceed the negotiated bearer(s) capacities.

NOTE: In the case of Small Size 5G Core, PCF services may be applicable depending on procurer requirement based on deployment scenario.

3.8.1 PCF functional requirements:

a. The PCF shall support:

i). Interactions with the access and mobility policy enforcement in the AMF, through service-based interfaces.

ii). Decision taking based upon subscription information, Access Type and the RAT Type.

iii). Handling of UE Context Establishment request as a part of UE Registration.

iv). The capability to take a PCC rule into service, and out of service, at a specific time of day.

v). Session management related functionality of PDU Session related policy control.

vi). The capability to indicate to the SMF that a PCC rule shall be bound to the specified QoS flow (including default QoS flow).

vii). Control of QoS for the packet traffic of the PDU Session.

viii). Mechanism to initiate QoS Flow establishment and modification as part of the QoS control.

b. Handling QoS Flows that require a guaranteed bitrate (GBR bearers) and QoS Flows for which there is no guaranteed bitrate (non-GBR bearers).

c. The PCF may support:

i). Utilization of the locally configured operator policies to make authorization and policy decisions, if the UE IP address belongs to an emergency DNN. The PCF shall not perform subscription check in this case.

ii). Charging control, policy control or both for a DNN access.

iii). Session management related functionality of Policy and charging control for a service data flow.

iv). Selective Blocking of RCS Services based on PLMN, TAI and Postpaid/Prepaid Subscription.

v). SmPolicyDecision data structure to provide the revalidation time within the "revalidationTime" attribute and the RE_TIMEOUT policy control request trigger within the "policyCtrlReqTriggers" attribute to instruct the SMF to trigger a PCF interaction to request PCC rule from the PCF as per 3GPP TS 23.503.

vi). During the lifetime of the PDU session, within the SmPolicyDecision data structure, the PCF may provide the revalidation time within the "revalidationTime" attribute and the RE_TIMEOUT policy control request trigger within the "policyCtrlReqTriggers" attribute to instruct the SMF to trigger a PCF interaction to request PCC rule from the PCF, if not provided yet.

vii). Session binding, which shall take the following IP CAN parameters into account:

1. The UE IPv4 address and/or IPv6 network prefix;
2. The UE identity, if present; and
3. The information about the packet data network (PDF) the user is accessing, if present.

viii). Data barring based on PLMN and TAC (Type allocation code in IMEI);

ix). Modification of the authorized Session AMBR at any time during the lifetime of the PDU session and provision it to the SMF; and

x). Modification of the authorized Default QoS during the lifetime of the PDU session and provision it to the SMF.

xi). Roaming - Communication with H-PCF over N24 interface for obtaining relevant UE Policy via SEPP.

3.9 NEF (Network Exposure Function)

NEF provides a means to securely expose the services and capabilities provided by 3GPP Network Functions.

NOTE: In the case of Small Size 5G Core, NEF services may be applicable depending on procurer requirement based on deployment scenario.

3.9.1 NEF functional requirements:

a. The NEF shall be connected with other 3GPP network elements using standard Service based interface
   i). NRF;
   ii). BSF;
   iii). PCF, N30; and
   iv). AF, N33.
b. The NEF shall support:
   i). Service-based interface Nnef;
c. The NEF may support:
   i). Masking of network and user sensitive information to external AF's according to the network policy.
   ii). Procedure for resource management of Background Data Transfer (BDT).

iii). Resource Management of BDT API for background data transfer.

iv). Nnef_TrafficInfluence service, Nnef_AFsessionWithQoS service

v). Authentication of the Application Functions, authorization of Application Functions, throttling of the Application Functions, exposure of monitoring capabilities, exposure of provisioning capabilities, policy/charging capabilities.

vi). Sending a GET request to the UDM to receive the SUPI that corresponds to the provided GPSI. The request contains the UE's identity (GPSI) and the type of the requested information.

vii). Nnef_BDTPNegotiation service, Nnef_ChargeableParty service, NF_management operations with NRF, exposure of bulk subscription.

viii). Translation of information exchanged with the AF and information exchanged with the internal network function.

d. NEF may be connected to UDR, using standard Service based interface N37.

3.10 NSSF (Network Slicing Selection Function)

NSSF provides a solution to select the optimal network slice available for the service requested by the user in the 5G environment, where various services are provided.

NOTE: In the case of Small Size 5G Core, NSSF services may be applicable depending on procurer requirement based on deployment scenario.

3.10.1 NSSF functional requirements:

a. NSSF shall be connected with other 3GPP network elements, viz. NRF and AMF, using Standard Service-based Interface.

b. NSSF may be connected with other 3GPP network elements, viz. EMS using Standard Service-based Interface

c. The NSSF shall support:

i). Determination of the Allowed NSSAI.

ii). single UE access to one or more Network Slice Instance

iii). Selection of same AMF for different set of slices.

iv). Nnssf_NSSelection for slice-info-request-for-registration to provide the Allowed NSSAI, configured NSSAI and may provide AMF set or the list of candidate AMF information to the Requester in Roaming scenarios and, if needed, mapping to the Subscribed S-NSSAIs.

v). Provision of configured slice information for the PLMN when requested with “default configured S-NSSAI “indication.

vi). Availability Service to provide AuthorizedNssaiAvailabilityInfo slice that is available per TAI for the S-NSSAIs the NF service consumer supports.

vii). Following services:

1. NFRegister service;
2. NFDeregister service; and
3. NFStatusNotify service.

d. The NSSF may support following services:

i). NFStatusSubscribe service; and

ii). NFProfileRetrieval service.

e. NSSF may support

i). Nnssf_NSSAIAvailability delete service operation for deletion of availability of S-NSSAIs per TA.

ii). The capability to provide bulk provisioning over all exposed interfaces. It shall provide Real time subscriber data synchronization.

iii). Roaming - Communication with the H-NSSF for selection of the S-NSSAI applicable in the case of roaming.

3.11 BSF (Binding Support Function)

BSF is used for binding an application-function request to a specific PCF instance.

NOTE: In the case of Small Size 5G Core, BSF services may be applicable depending on procurer requirement based on deployment scenario.

3.11.1 BSF functional requirements:

a. The BSF shall be compliant with 3GPP TS 29.521 “Binding Support Management service”.

b. The BSF shall support:

i). Registration of BSF profile with NRF, if NRF is available/part of the 5G compact mobile system.

ii). heartbeat procedure periodically with NRF to update NF status. This heartbeat message shall also include BSF load information, if NRF is available/part of the 5G compact mobile system.

iii). Discovery of BSF via Nnrf_Discovery API by the NF Consumers (NEF or AF), if NRF is available/part of the 5G compact mobile system.

iv). Creation, storage, updation and deletion of session binding information with various parameters such as UE address, PCF ID, DNN, SUPI or S-NSSAI.

v). Binding between PCF and NEF or AF.

3.11.2 BSF QoS requirements

a. The BSF shall support:

i). Use of Nbsf_Management_Register, Nbsf_Management_Deregister and Nbsf_Management_Update service operations by PCF; and

ii). Nbsf_Management_Register, Nbsf_Management_Deregister and, Nbsf_Management_Update to register, deregister and update binding information into the BSF.

iii). Use of Nbsf_Management_Deregister service operation to delete binding information when Policy Association Termination is initiated by the SMF and PCF.

iv). Use of Nbsf_Management_Deregister service operation to delete binding information when Policy Association Termination is initiated by the PCF.

b. The BSF may support:

i). Use of Nbsf_Management_Discovery service operation to obtain the selected PCF id for a PDU session by a client NEF, NWDAF, AF, IMS,

DRA). BSF responds with the PCF id and others related binding information.

3.12 CHF (Charging Function)

CHF allows charging services to be offered to authorized network functions.

NOTE: In the case of Small Size 5G Core, CHF services may be applicable depending on procurer requirement based on deployment scenario.

3.12.1 CHF functional requirements:

a. The CHF shall support:

i). Following charging features:

1. Usage based charging;
2. Speed based charging/ Quality of service charging;
3. Application ID charging;
4. Network slice-based charging on 5G;
5. URL based charging.

ii). converged online charging and offline charging functionalities. The CHF provides the following:

1. Quota;
2. Re-authorization triggers;
3. Receiving service usage reports from NF Service Consumer; and
4. CDRs generation.

iii). N40 interface with the SMF for Data Connectivity Charging, which includes:

1. Flow based charging (FBC); and
2. QoS Flow based Charging (QBC).

iv). Time-based, volume-based and event-based charging and any such combination.

v). 3GPP specified services;

vi). Consumption of services exposed by the NRF;

vii). 5G defined new identities: GPSI (MSISDN) and SUPI (IMSI);

viii). Charging based on supported 5G network architectures such as Multiple IP Address, Multiple Slices, Multiple Identifiers across Networks, No phone number, on-net vs roaming, etc;

ix). Charging Data Record (CDR) file format and transfer and Charging Data Record (CDR) parameter description as per 3GPP specifications. The output CDR format may be compliant to ASN.1 structure as per 3GPP specification; and

x). Upgradeability to 3GPP Rel-16 functionality and also backward compatibility;

xi). All mandatory fields for CDR in 3GPP TS32.255;

xii). Nchf_ConvergedCharging request message containing different multipleUnitUsage information and reply with multipleUnitInformation, associated to several Rating Groups being accessed during the PDU session and which may be managed with different charging methods (online or offline).

xiii). Charging of roaming traffic.

xiv). Following interface functions from CHF perspective:

xv). Support Interface with AMF/SGSN/MME/SMF/UPF/SPGW; and

xvi). CHF to Register/update/deregister towards NRF.

xvii). Converged online and offline charging triggered from Session Management Function (SMF).

xviii). Following notification requirements –

xix). Nchf_ConvergedCharging_Create/Delete /Notify; and

xx). Nchf_SpendingLimitControl_Subscribe/Unsubscribe/Notify.

xxi). Different charging between 4G and 5G.

b. The CHF may support:

i). Charging of 5G sessions in case of session and service continuity mode, as defined in TS 32.255.

ii). Spending Limit Control Service of the Nchf Service according to TS 32.290 and TS 29.504

3.12.2 CHF QoS requirements:

a. The CHF shall support:

i). QoS flow-based Charging (QBC), where data volumes are collected per user and per PDU session and categorized per QoS Flow identified by its QoS Flow Identifier (QFI).

ii). Flow-based charging (FBC) where data volumes are collected per user and per PDU session and categorized per rating group or per combination of rating group/service identifier related to one or more individual service data flows.

iii). Integration of 4G Charging and 5G charging.

iv). Charging of services based on network slice, as well as charging as per network slice management.

v). PDU session charging (data volumes are collected per user and per PDU session).

3.13 SMSF (Short Message Service Function)

SMSF is required for the provision of SMS over NAS through AMF. Optionally, SMS service may be offered through use of IMS.

NOTE: In the case of Small Size 5G Core, SMSF services may be applicable depending on procurer requirement based on deployment scenario.

a. The SMSF may support convergent charging towards CHF.

3.14 NWDAF (Network Data Analytics Function)

NWDAF is a NF used to collect data from user equipment, network functions, and operations, administration, and maintenance (OAM) systems, etc.

NOTE: In the case of Small Size 5G Core, NWDAF services may be applicable depending on procurer requirement based on deployment scenario.

a. The NWDAF shall support one or more of the following functionalities:
   i). Identifier of network slice instance.
   ii). load level information for that network slice instance.
   iii). Support data collection from NFs and AFs.
   iv). Support data collection from OAM.
   v). NWDAF service registration and metadata exposure to NFs and Afs.
   vi). Support analytics information provisioning to NFs and AFs.
   vii). Support Machine Learning (ML) model training and provisioning to NWDAFs (containing Analytics logical function).
b. The NWDAF may allow NF consumers to subscribe to and unsubscribe from periodic notification and/or notification when a threshold is exceeded.

3.15 SEPP (Security Edge Protection Proxy)

SEPP is required to manage the connectivity in trusted mode and to ensure that the exchange of information (signalling) among Operators may take place in a confidential, secure and robust way, aiming to protect against malicious attempts or attacks on data confidentiality, identity spoofing or information tampering.

NOTE: In the case of Small Size 5G Core, SEPP services may be applicable depending on procurer requirement based on deployment scenario.

a. The SEPP is a non-transparent proxy and shall support:
   i). Message filtering and policing on inter-PLMN control plane interfaces.
   NOTE: The SEPP protects the connection between Service Consumers and Service Producers from a security perspective, i.e., the SEPP does not duplicate the Service Authorization applied by the Service Producers.
   ii). Topology hiding. The SEPP applies the functionality to every Control Plane message in inter-PLMN signalling, acting as a service relay between the actual Service Producer and the actual Service Consumer. For both Service Producer and Consumer, the result of the service relaying is equivalent to a direct service interaction. Every Control Plane

message in inter-PLMN signalling between the SEPPs may pass via IPX entities.

iii). N32 interface

3.16 SCP (Service Communication Proxy)

SCP is the routing control point that mediates all Signalling and Control Plane messages in the network core.

NOTE: In the case of Small Size 5G Core, SCP services may be applicable depending on procurer requirement based on deployment scenario.

a. The SCP shall support load balancing, monitoring, overload control etc.
b. The SCP includes one or more of the following functionalities:
   i). Indirect Communication;
   ii). Delegated Discovery;
   iii). Message forwarding and routing to destination NF/NF service; and
   iv). Message forwarding and routing to a next hop SCP.

NOTE: Some or all of the SCP functionalities may be supported in a single instance of an SCP:

c. The SCP may support communication security (e.g. authorization of the NF Service Consumer to access the NF Service Producer API).

3.17 N3IWF (Non-3GPP Interworking Function)

N3IWF acts as a gateway for the 5GC with support for N2 and N3 interface towards the 5GC.

NOTE: In the case of Small Size 5G Core, N3IWF services may be applicable depending on procurer requirement based on deployment scenario.

a. The N3IWF shall support:
   i). 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.

ii). Termination of N2 and N3 interfaces to 5G Core Network for control - plane and user-plane respectively.

iii). Relaying uplink and downlink control-plane NAS (N1) signalling between the UE and AMF.

iv). Handling of N2 signalling from SMF (relayed by AMF) related to PDU Sessions and QoS.

v). Establishment of IPsec Security Association (IPsec SA) to support PDU Session traffic.

vi). Relaying uplink and downlink user-plane packets between the UE and UPF. This involves:

1. De-capsulation/ encapsulation of packets for IPSec and N3 tunnelling;
2. 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;
3. Local mobility anchor within untrusted non-3GPP access networks using MOBIKE per IETF RFC 4555;

3.18LMF

The LMF manages the overall co-ordination and scheduling of resources required for the location of a UE that is registered with or accessing 5GCN. It also calculates or verifies a final location and any velocity estimate and may estimate the achieved accuracy.

NOTE: In the case of Small Size 5G Core, Location services may be applicable depending on procurer requirement based on deployment scenario.

a. The LMF shall:

i). determine the result of the positioning in geographical co-ordinates as defined in TS 23.032. If requested and if available, the positioning result may also include the velocity of the UE.

b. The LMF may support:

i). request for a single location received from a serving AMF for a target UE.

ii). request for periodic or triggered location received from a serving AMF for a target UE.

iii). Determination of position methods based on UE and PLMN capabilities, QoS, UE connectivity state per access type and LCS Client type.

iv). Report of UE location estimates directly to a GMLC for periodic or triggered location of a target UE.

v). cancelation of periodic or triggered location for a target UE.

vi). provision of broadcast assistance data to UEs via NG-RAN in ciphered or unciphered form and forward any ciphering keys to subscribed UEs via the AMF.

vii). change of a serving LMF for periodic or triggered location reporting for a target UE.

3.19 CBCF

CBCF is used in Public Warning System (PWS) for cell broadcast of CBS messages and acts as manager between the Cell broadcast Entity that generates the message and the AMF that further transmits it to the UE through the NG-RAN.

NOTE: In the case of Small Size 5G Core, PWS services may be applicable depending on procurer requirement based on deployment scenario.

a. The CBCF shall support:

i). The CBCF shall be responsible for the management of CBS messages

ii). allocation of serial numbers;

iii). modifying or deleting CBS messages held by the NG-RAN node;

iv). initiating broadcast by sending fixed length CBS messages to a NG-RAN node for each language provided by the cell, and where necessary padding the pages to a length of 82 octets (see 3GPP TS 23.038 [3]);

v). determining the set of cells to which a CBS message should be broadcast, and indicating within the Serial Number the geographical scope of each CBS message;

vi). determining the time at which a CBS message should commence being broadcast;

vii). determining the time at which a CBS message should cease being broadcast and subsequently instructing each NG-RAN node to cease broadcast of the CBS message;

viii). determining the period at which broadcast of the CBS message should be repeated;

ix). when CBS transmits emergency messages, allocation of "emergency indication" to differentiate it from normal CBS messages.

CHAPTER 4

4 IP Multimedia Sub-system (IMS)

The IP Multimedia Subsystem (IMS) is a standardized Next Generation Network (NGN) architecture for enabling a mobile to use mobile and fixed multimedia services. IMS uses a number of Internet Protocol (IP)-based services viz. Voice over IP (VoIP), multi-party gaming, video-conferencing, Instant Messaging, community services, presence information and content sharing etc. based on standardized Session Initiation Protocol (SIP) implemented by 3rd Generation Partnership Project (3GPP). SIP is used for the realtime, peer-to-peer, multi-party and multi-media capabilities of IMS. Service control, security functions, routing, registrations, charging, SIP compression and QoS support may be achieved through necessary IMS capabilities

The Small Size 5G Core System may have:

a. IMS functionality for supporting SMS.
b. IMS functionality for Voice and Video Service over 5G Network.
c. SIP & RTP interface for external interface towards IP PABX/ MGW for voice interworking etc.

CHAPTER 5

5 OMC/ EMS requirements

The OMC allows centralized operation of the various units in the system and functions needed to maintain the sub-systems. The OMC provides the dynamic monitoring and controlling of the network management functions.

5.1 Management Functions

a. Configuration management
b. Fault report and alarm handling
c. Performance supervision/management
d. Storage of system software and data
e. Security management

5.2 OMC database

a. The OMC shall use the relational/object-oriented database to store and hold the necessary information for the parameters used in the OMC.
b. The OMC database shall include configuration data, maintenance data, fault data and performance / QoS data
c. The database in the OMC shall reside in a disk with mirroring capability.
d. The OMC shall be capable of storage of the generated performance data. The methods and capacity of storage provided with the system shall be stated.
e. Provision shall be available for collection of statistical information relating to events in the network. Collection frequency shall be configurable
f. The OMC database shall contain the fault history of the whole network under its command. As a minimum, it shall be possible to search and display data according to the following criteria: -Network elements,-Severity class,-Event type.

5.3 OMC Generic Features

a. OMC software – UNIX/LINUX/Windows System Platform
b. It shall optionally support interface like CORBA / TCP / IP / CMIP /
c. SNMP/ REST / HTTP etc., to enable it to work with a remote NMS.
d. Support Ethernet connectivity with remote network elements.
e. Graphical User Interface (GUI). Or Management
   through Element Management System
f. On-Line Help.
g. Consistency Checks.
h. Configuration Change/Event Log.
i. Object Alarm Status Management / Display.
j. Collection of PM counters.
k. Limited Access Restriction by User.
l. Access Restriction by Function and by Operation.

CHAPTER 6

6 Generic Common Requirements

6.1 Operation and Maintenance

This section identifies generic O&M requirements to be implemented by the network functions.

a. The NFs shall provide a flexible & secure management interface for configuration, fault management and performance management.
b. The NFs shall include an O&M interface for debugging and troubleshooting.
c. NFs shall support at least one of the following interfaces towards EMS
    i). SNMP
    ii). REST
    iii). HTTPS
d. For performance management, the node shall generate various performance counters and provide mechanism to transfer the same to external entity for further analysis.
e. Fault Report and Alarm Handling
    i). For fault management, the NFs shall support Event Based Monitoring where all events will be streamed out of the NF and available for external processing.
    ii). Fault Management system shall have the ability to detect and mitigate or recover from faults.
f. Alarm Surveillance

Alarms shall be raised for adverse events in the network. The information included in the alarms shall be detailed enough to identify which system component is experiencing the failure condition. The detail shall include

i). Alarm type

ii). The probable cause

iii). The specific problem

iv). The perceived severity

v). Network Element ID

vi). Network Element Type

g. The alarms shall be automatically cleared when the failure condition is resolved. It shall not record or forward duplicate alarms for detection of the same failure condition.

h. The NF shall support software upgrade.

i. The NF may support Software resiliency in disaster and temporary deployment for enabling automatic recovery with minimal human intervention using stateless microservices and redundant storage.

j. The system may support scalability features to accommodate varying demands in disaster and temporary deployments efficiently.

k. The control software shall be responsible for logging and sending the log file on the network to a designated syslog server.

l. The system shall maintain a system log and core dump logs.

m. The NF shall support alarms, events to OMC for visual indicators of status and fault.

n. The NF shall have reboot and shut-down capability.

o. The NF may be capable of providing the system configuration data to the Management Information Base (MIB) of the system (applicable with SNMP based management only).

CHAPTER 7

7 General Requirements

7.1 Software Requirements

a. Modular, structured software written in High-Level Language
b. Software easy to handle during installation and normal operations as well as during extensions
c. Introduction of changes in software, wherever necessary, with least impact on other modules
d. Open-ended to allow addition of new features
e. Adequate flexibility to easily adopt changes in service features & facilities and technological evolution in hardware
f. Propagation of software faults is contained
g. Test programs to include fault tracing for detection and localization of system faults

7.2 Software Maintenance Requirements

a. Continuous supply of all software updates, for the period specified
b. Integration of software updates without posing any problem to the existing functionality

CHAPTER 8

8 INFORMATION FOR THE PROCURER OF PRODUCT

Interfaces and features which are optional needs to be examined by the procurer and suitably specified in the tender conditions as per their requirement based on the deployment scenario specific to the procurer and mentioned in the following tabular format and these will be used for type approval.

Similarly, for a vendor applying for the Technology approval, the Interfaces and features which are optional needs to be examined by the vendor and suitably specified as per their requirement based on the deployment scenario envisioned by the vendor and mentioned in the following tabular format.

8.1 List of NFs supported

S. No.	NF	Supported/Not Supported
a)	AMF	
b)	SMF	
c)	UPF	
d)	AUSF	
e)	UDM	
f)	UDR	
g)	NEF	
h)	NRF	
i)	NSSF	
j)	PCF	

k)	CHF	
l)	BSF	
m)	SMSF	
n)	NWDAF	
o)	SEPP	
p)	SCP	
q)	N3IWF	
r)	LMF	
s)	CBCF	

8.2 List of optional Clauses supported

S. No.	**NF**	**Clause No.**
a)	SMF	3.2.1. c. , 3.2.2. a.
b)	UDM	3.4.1. c., 3.4.1. d.
c)	UDR	3.6.1. c.
d)	SMSF	3.13
e)	NWDAF	3.14
f)	SEPP	3.15
g)	SCP	3.16
h)	N3IWF	3.17
i)	LMF	3.18

j)	CBCF	3.19

8.3 Support for broad level features

S. No.	Parameter	Option
a)	Targeted use case - eMBB	Yes/No
b)	Targeted use case - URLLC	Yes/No
c)	Targeted use case - mMTC	Yes/No
d)	Roaming	Yes/No
e)	Location services	Yes/No
f)	Public Warning System	Yes/No
g)	Mission critical features	Yes/No
h)	Support for IMS	Yes/No
i)	Support for network slice	Yes/No
j)	Support for non conventional energy source If Yes, mention type and Rating.	Yes/No

8.4 Dimensioning

S. No.	Parameter	Value
a)	Support for number of configured subscribers	
b)	Support for number of active subscribers	

c)	Support for aggregate data speed	

ABBREVIATIONS

For the purpose of this document the following abbreviations apply:

5G-AKA 5G Authentication and Key Agreement

5GC 5G Core Network

5G-EIR 5G Equipment Identity Register

5GS 5G System

5QI 5G QoS Identifier

AANF AKMA Anchor Function

ADR Advanced RF Technologies

AF Application Function

AMBR Aggregate Maximum Bit Rate

AMF Access and Mobility Management Function

AUSF Authentication Server Function

BDT Background Data Transfer

BSF Binding Support Function

CBCF Cell Broadcast Centre Function

CHF Charging Function

CLI Command Line Interface

CP Control Plane

CPU Central Processing Unit

DCCF Data Collection Coordination Function

DL Downlink

DN Data Network

DSCP Differentiated Services Code Point

EASDF Edge Application Server Discovery Function

FBC Flow Based Charging

GBA Generic Bootstrapping Architecture

GBR Guaranteed Bit Rate

GPSI Generic Public Subscription Identifier

GMLC Gateway Mobile Location Centre

HSS Home Subscriber Server

HTTP Hypertext Transfer Protocol

IMS IP Multimedia Subsystem

I-UPF Intermediate UPF

IP Internet Protocol

LAN Location Area Network

LCS Location Services

LMF Location Management Function

mIoT massive Internet of Things

MB-SMF Multicast/Broadcast-SMF

MBSF Multicast/Broadcast Service Function

MFBR Maximum Flow Bit Rate

MFAF	Messaging Framework Adapter Function
NEF	Network Exposure Function
NF	Network Function
NG-RAN	Next-Generation Radio Access Network
NR	New Radio
NRF	Network Repository Function
NSACF	Network Slice Access Control Function
NSSF	Network Slice Selection Function
NSSAAF	Network Slice Specific Authentication and Authorization Function
NSWOF	Non-Seamless WLAN Offload Function
NWDAF	Network Data Analytics Function
OAM	Operations, Administration, and Maintenance
P-CSCF	Proxy-Call Session Control Function
PCF	Policy Control Function
PEI	Permanent Equipment Identifier
PLMN	Public Land Mobile Network
PDU	Protocol Data Unit
PWS	Public Warning System
QFI	QoS Flow Identifier
QoS	Quality of Service
RAN	Radio Access Network

RAT Radio Access Technology

SBA Service-Based Architecture

SBI Service Based Interface

SCP Service Communication Proxy

SEPP Security Edge Protection Proxy

SMF Session Management Function

SMSF Short Message Service Function

SNPN Stand-alone Non-Public Network

SUPI Subscription Permanent Identifier

SUCI Subscription Concealed Identifier

TAC Tracking Area Code

TAI Tracking Area Identity

TCP Transmission Control Protocol

TTL Time-To-Live

TSCTSF Time Sensitive Communication Time Synchronization Function

UDM Unified Data Management

UDR Unified Data Repository

UDSF Unstructured Data Storage Function

UE User Equipment

UL Uplink

URLLC Ultra Reliable Low Latency Communication

URRP-AMF UE Reachability Request Parameter for AMF

URR Usage Reporting Rules

UPF User Plane Function

VPLMN Visited Public Land Mobile Network

======== End of the document ========