वर्गीय आवश्यकताओं के लिए मानक टी.ई.सी

२२१६०:२०२६

STANDARD FOR GENERIC REQUIREMENTS

TEC 22160:2026

5जी कोर

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

Release2: XXXX, 2026

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 Generic Requirements (GR) of the 5G Core based mobile system suitable for 5G SA (Stand alone) deployment in the Indian mobile communication networks.

It specifies Technical Requirements, General Requirements, Features and Functionality including OMC/EMC Requirements and Security Requirements of the 5G Core based mobile system.

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

Sl. No.	GR No.	Title	Remarks
01	TEC 22160:2023	Standard for Generic Requirement for 5G Core	New GR

REFERENCES

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. Scope

This document specifies Technical Requirements, General Requirements, Features and Functionality of the various 5G core network functions viz. AMF, SMF, UPF, AUSF, UDM,UDR, NEF, NRF, NSSF, PCF, CHF, BSF, SMSF, NWDAF, SEPP, SCP, N3IWF, LMF, GMLC, UDSF, NSACF, NSSAAF, AANF, UCMF, MFAF, MB-SMF, ADRF, DCCF, MBSF, TSCTSF, 5G-EIR, TNGF, TWIF and AF and OAM system for deployment in the Indian mobile network. The network functions (NFs) have been classified into mandatory and optional as below:

Mandatory NFs: AMF, SMF, UPF, AuSF, UDM, NSSF, PCF, CHF, BSF, NRF

Optional NFs: UDR, NEF, SMSF, NWDAF, DCCF, ADRF, MFAF, SEPP, SCP, N3IWF, LMF, GMLC, UDSF, NSACF, NSSAAF, AANF, UCMF, MB-SMF, MBSF, TSCTSF, 5G-EIR, TNGF, TWIF and AF

Note: The certification against this GR will mention the list of all mandatory NFs and list of those optional NFs against which testing has been conducted as per test guide.

Chapter 2

2. 5G Core

2.1. Architecture

The key components of the 5G Core architecture that are part of the scope of this document are as mentioned below:

a) Access and Mobility Management Function (AMF).
b) Session Management Function (SMF).
c) User Plane Function (UPF).
d) Authentication Server Function (AUSF).
e) Unified Data Management (UDM).
f) Unified Data Repository (UDR).
g) Network Exposure Function (NEF).
h) Network Repository Function (NRF).
i) Network Slice Selection Function (NSSF).
j) Policy Control Function (PCF).
k) Charging Function (CHF).
l) Binding Support Function (BSF).
m) SMS Function (SMSF)
n) NWDAF (Network Data Analytics Function)
o) DCCF ((Data Collection Coordination Function)
p) ADRF (Analytics Data Repository Function)
q) MFAF (Messaging Framework Adaptation Function)
r) SEPP (Security Edge Protection Proxy)
s) SCP (Service Communication Proxy)
t) N3IWF (Non-3GPP Interworking Function)LMF (Location Management Function)
u) GMLC (Gateway Mobile Location Centre)
v) UDSF (Unstructured Data Storage Function)
w) NSACF (Network Slice Admission Control Function)

x) NSSAAF (Network Slice Specific Authentication and Authorization Function)

y) AANF (AKMA Anchor Function)

z) UCMF (UE Radio Capability Management Function)

aa) MB-SMF (Multicast Broadcast Session Management Function)

bb) MBSF (Multicast Broadcast Service Function)

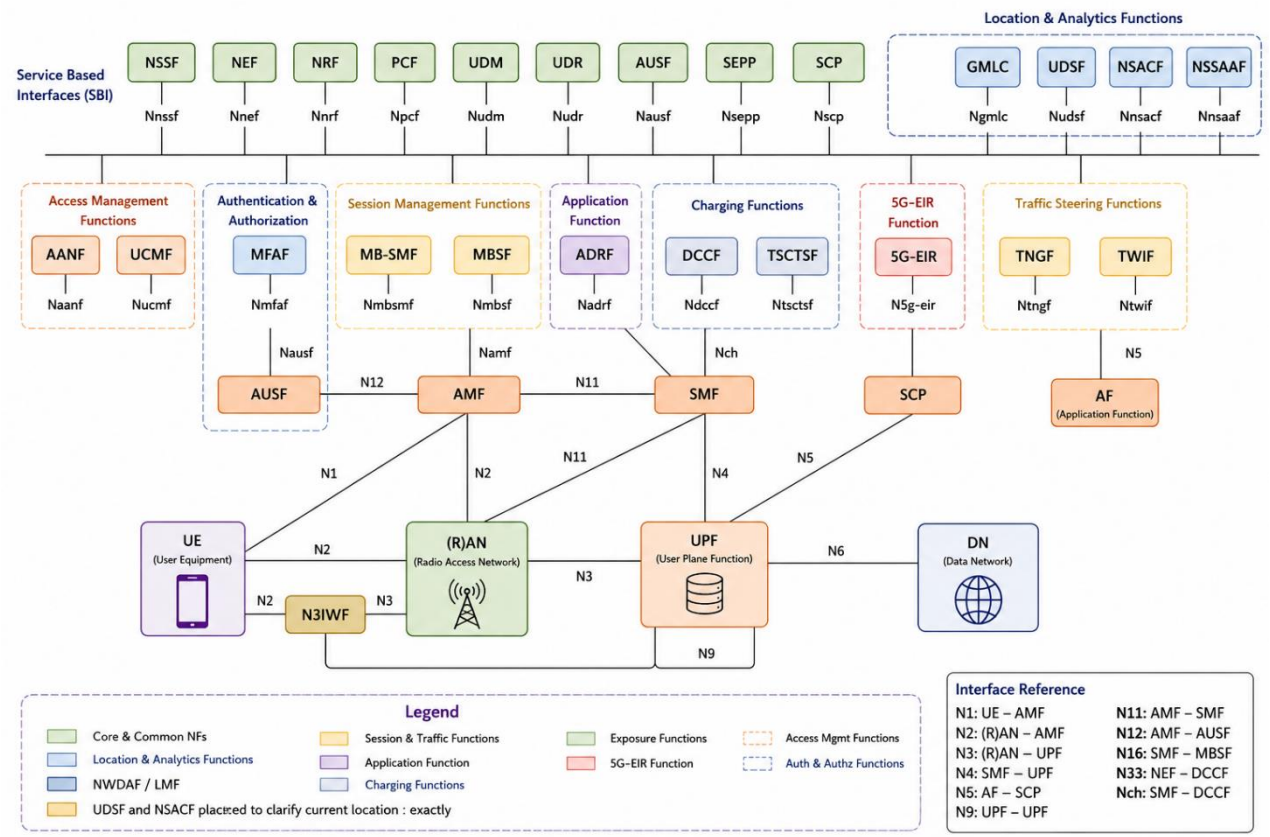
cc) TSCTSF (Time Sensitive Communication Time Synchronization Function)

dd) 5G-EIR (5G-Equipment Identity Register)

ee) TNGF (Trusted Non-3GPP Gateway Function)

ff) TWIF (Trusted WLAN Interworking Function)

gg) Application Function (AF)



The new 5G core, as defined by 3GPP, utilizes cloud-aligned, service-based architecture (SBA) that spans across all 5G functions and interactions including authentication, security, session management and aggregation of traffic from end devices.

2.1.1. Interfaces for 5G Core network:

This section describes an exhaustive list of 5G System service-based interfaces. The applicability of an interface to a specific 5G Core category is defined in node specific sections.

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 Boostrapping Server Function in GBA.

Neasdf: Service-based interface exhibited by EASDF.
Nlmf: Service-based interface exhibited by LMF.
Ngmlc: Service-based interface exhibited by GMLC.
Ntngf: Service-based interface exhibited by TNGF.
Ntwif: Service-based interface exhibited by TWIF.
N5g-eir: Service-based interface exhibited by 5G-EIR.
Naanf: Service-based interface exhibited by AANF.

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.
Nmbsmf: Service-based interface exhibited by MB-SMF.
Nmbsf: Service-based interface exhibited by MBSF.
Ntsctsf: Service-based interface exhibited by TSCTSF.
Nnsacf: Service-based interface exhibited by NSACF.
Nnssaaf: Service-based interface exhibited by NSSAAF.
Nudsf: Service-based interface exhibited by UDSF.

2. Reference points

The 5G System Architecture contains the following reference points:

N1: Reference point between the UE and the AMF.

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

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

N4: Reference point between the SMF and the UPF.

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

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.

N26: Reference point between AMF and MME

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.

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 3GPP TS 23.503.

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.

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)

3.1.1. AMF functional requirements:

3.1.1.1. The AMF shall be capable of connecting to

(a) NG-RAN;

(b) SMF;

(c) PCF;

(d) UDM; and

(e) AUSF

3.1.1.2. The AMF shall support:

(a) Registration management, connection management, reachability management and mobility management for the UE.

(b) AUSF selection based on NRF query for UE authentication;

(c) Primary authentication with AUSF using SUCI and SUPI for 5G AKA with SBI;

(d) Control Plane signaling confidentiality and integrity protection of NAS signaling;

(e) Transport for Session Management (SM) NAS messages between UE and SMF and act as a transparent proxy for routing SM messages.

(f) Network initiated PDU session release procedure when the UE is in idle state;

(g) UE initiated PDU session release procedure in connected state;

(h) UE triggered service request procedure and respond with a service request message;

(i) Xn based inter NG-RAN Handover;

(j) Inter NG-RAN node N2 based handover;

(k) EPS bearer ID allocation for interworking with EPS;

(l) 5GS to EPS & EPS to 5GS handover using N26 interface;

(m) Idle mode mobility procedure from 5GS to EPS & EPS to 5GS;

(n) Provision of PEI (Permanent Equipment Identifier) of the UE to the SMF if the PEI is available with the AMF at the time of PDU session establishment

(o) Act as the Security Anchor Function (SEAF), interacting with AUSF and UE.

(p) Support paging of the UE, including paging-profile based paging optimisation and paging retransmission

3.1.1.3. AMF may support:

(a) SMF selection based on DNN.

(b) Rejecting PDU session establishment based on SUPI and DNN;

(c) Xn based handover with insertion of intermediate SMF;

(d) Xn based handover with re-allocation of intermediate SMF;

(e) Xn based handover with removal of intermediate SMF;

(f) Setting of the IWK N26 bit to "interworking without N26 not supported" if the AMF does not support interworking procedures without N26 interface.

3.2. SMF (Session Management Function)

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

3.2.1. SMF functional requirements:

3.2.1.1. The SMF shall be capable of connecting to the

(a) AMF;

(b) UPF;

(c) PCF;

(d) UDM; and

(e) CHF.

3.2.1.2. The SMF shall support:

(a) Session establishment between UPF and NG-RAN node;

(b) Selection and control of UPF function;

(c) Converged online and offline charging;

(d) Charging of PDU session using SBI interface;

(e) CHF selection based on the Charging Characteristics or using NRF;

(f) Starting new counts with time stamp on expiry of time limit per PDU session if the PDU session is still active;

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

(h) Starting new counts with time stamp on expiry of data volume limit per PDU session if the PDU session is still active;

(i) Deletion of the UE PDU session when it receives the request

(a) The cause IE set to "REL_DUE_TO_DUPLICATE_SESSION_ID" from AMF; and

(b) The cause IE set to "REL_DUE_TO_SLICE_NOT_AVAILABLE" from AMF.

(j) Allocation of static IPv4 and/or static IPv6 prefix based on subscription information received from UDM.

(k) Determine the Session and Service Continuity (SSC) mode for a PDU session

(l) Differentiate and support local-breakout and home-routed roaming scenarios for PDU sessions.

(m) Reflective QoS control at the session level, instructing the UPF to set the RQI accordingly

3.2.2. SMF QoS requirements:

3.2.2.1. The SMF shall support:

(a) QOS and Policy enforcement;

(b) QoS handling on Flow level, Service level as well as Session level;

(c) Both Default QoS flows as well as Dedicated QoS flows;

(d) Both pre-configured and dynamically assigned 5QI;

(e) 5QI values in the range of 1-254;

(f) operator-specific 5QI in the range of 128-254; and

(g) Upto 16 QoS flows per UE.

(h) Inclusion of GBFR and MFBR in QOS Profile for each GBR QoS Flow

(i) Conversion of operator-specific 5QIs or QCIs to 3GPP-specified 5QIs or QCIs for N1 messages.

3.2.2.2. The SMF may support:

(a) packet marking for HTTP/2 signaling over SBI.

(b) UE IP address allocation and management;

(c) Both a local and central UPF within a PDU session;

(d) Sending of Charging Data Request [Termination] when abort request is received from the CHF;

(e) 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.

(f) 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;

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

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 (5GC).

3.3.1. UPF functional requirements:

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

(a) SMF;

(b) NG-RAN;

(c) Data Network; and

(d) Peer UPF.

3.3.1.2. The UPF shall support:

(a) Packet Detection based on predefined PDRs or PDRs received in the PFCP messages from the SMF over N4 interface;

(b) A PDU session that carries IPv4, IPv6 traffic;

(c) QoS Flow ID (QFI) used to identify a QoS flow;

(d) User Plane Traffic to QoS flows based on the SDF templates;

(e) Buffering of packets instead of immediately forwarding them based on the instructions received from the control plane;

(f) Serve as the external PDU-session point of interconnect to the Data Network

(g) QoS Flow-to-DRB mapping enforcement in the downlink, as instructed by the SMF.

(h) Multi-Access PDU (MA PDU) Session user-plane functionality, including low-layer ATSSS traffic steering where deployed.

(i) Sending User Plane Inactivity Report to the SMF as a response when instructed;

(j) User Traffic Redirection based on

1. URI-based redirection; and
2. Destination IP.

(k) N4 session level report procedure:

1. Usage Report;

2. Start of traffic detection;
3. Stop of traffic detection; and

4. Detection of PDU session inactivity for a specified period.

3.3.1.3. The UPF may support:

(a) Application detection;

(b) 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;

(c) Tethering detection based on TTL values;

(d) Multi-homed PDU session;

(e) HTTP Pipelining Request-Response matching enabling the user plane to match each HTTP response with the corresponding HTTP request; and

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

(g) Monitoring the amount of downlink traffic that is dropped and report when a threshold is received as per the URR received from the SMF;

3.3.2. UPF QoS requirements:

3.3.2.1. The UPF shall support:

(a) Following QoS flows:

1. Guaranteed flow bit rate QoS flows; and
2. Non-guaranteed flow bit rate QoS flows.

(b) Transport level packet marking with a DSCP value.

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

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

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

(f) Marking of PDU session containers over the N3 and N9

interfaces with a QFI value that the control plane provides in a QER (QoS Enforcement Rule).

3.3.2.2. The UPF may support inclusion of QFI and an indication for reflective QoS activation in the encapsulation header.

3.4. UDM (Unified Data Management)

Unified data management (UDM) is a centralized way to control network user data.

3.4.1. UDM functional requirements:

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

(a) SMF, N10;

(b) AMF, N8;

(c) AUSF, N13;

(d) SMSF, N21; and

(e) GMLC, Nlh.

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

(a) UDR, N35; and

(b) HSS, Nhss;

3.4.1.3. The UDM shall support:

(a) Procedures of interworking with EPS based on N26 interface;

(b) Below mentioned high level features:

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

(c) UE Context Management function that allows HSS to trigger AMF deregistration upon UE mobility to EPC, as well as to trigger the P-CSCF restoration procedure.

(d) Maintenance of AMF/SMF registration session.

(e) Sending of deregistration notification using Nudm_UECM_DeregistrationNotification to NF consumer.

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

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

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

(i) Network-initiated deregistration requested by AMF using Nudm_UECM_DeregistrationNotification operation.

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

(k) User-identification handling, i.e. storage and management of the SUPI for each subscriber.

(l) Service/session continuity, e.g. by retaining SMF/DNN assignment for ongoing sessions.

(m) UE reachability status and event notifications to authorised NFs via Nudm_EventExposure

(n) Interworking with HSS

1. Network sharing and interworking between EPS and 5GS;
2. Terminating-Access Domain Selection for 5G access via UDM-HSS interworking; and
3. P-CSCF restoration via UDM-HSS interworking.

(o) Following Authentication related features:

1. Generation of 5G- AKA Authentication Credentials;
2. Selection of the 5G-AKA authentication method so that network Function Service Consumer (AMF) returns the result received from the UE to the AUSF;
3. Different protection scheme;

4. The EAP-based authentication method;

5. Support of de-concealment of privacy-protected subscription identifier (SUCI);

6. Support of MT-SMS delivery support services; and

7. MT-SMS delivery support for short Message Roaming Routing, Set Message Waiting Data, Report SM-Delivery Status.

(p) Following NRF services:

1. Nnrf_NFDiscovery service;

2. Nnrf_AccessToken service;

3. NFRegister, NFUpdate, NFDeregister service;

4. NF Heart-Beat service;

5. NFStatusSubscribe, NFStatusNotify, NFStatusUnSubscribe service;

6. NFListRetrieval service;

7. NFProfileRetrieval service;

8. Use of NF discovery service on expiry of validity Period; and

9. Validation of expire time present in token validation response from NRF.

3.4.1.4. The UDM may support:

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

(b) UDM may provide support to Service based interfaces for direct UDM-HSS interworking;

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:

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

(a) UDM, N13; and

(b) AMF, N12

(c) AuSF shall support secured communication with other NFs as per 3GPP TS 33.501 Clause 13.1.0

3.5.1.2. The AuSF shall support:

(a) UE authentication service to the requester NF using Nausf_UEAuthentication;
(b) Setting of the authResult to AUTHENTICATION FAILURE if the UE is not authenticated.
(c) Setting the authResult to AUTHENTICATION FAILURE if the UE is not authenticated.
(d) 5G-AKA procedures;
(e) UE id (e.g. SUPI or SUCI), Serving Network Name in the " authenticate" service request by NF; and
(f) 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 (EAP-AKA' procedure, if supported)
(g) Following NRF services:

1. Nnrf_NFDiscovery service;
2. NFRegister, NFUpdate and NFDeregister service;
3. NF Heart-Beat service;
4. NFStatusSubscribe service and NFStatusNotify service
5. NFStatusUnSubscribe service ;
6. NFListRetrieval service; and
7. NFProfileRetrieval service.

(h) 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.
2. AuSF shall validate expire time present in token validation response from NRF.

3.5.1.3. AuSF may support:

(a) EAP- AKA' procedures.

(b) Deletion of stale security context.

(c) Both On-demand as well as Periodic/Scheduled backup procedures;

(d) The system resource monitoring (CPU utilization, Memory Utilization etc.) through external server.

(e) Tracing functionality, that is, generating procedure level data records and sending those to a 'Records Collector', that is reachable on an IP address and Port.

(f) Authentication for 3GPP access and for untrusted non-3GPP access.

3.6. UDR (Unified Data Repository)

UDR enables network functions to store and access subscription information.

3.6.1. UDR functional requirements:

3.6.1.1. UDR shall be connected with other 3GPP network elements using standard service-based interface:

(a) UDM, N35;

(b) PCF, N25; and

(c) NEF, N37

3.6.1.2. The UDR shall support:

(a) Legacy access profile data like HSS /HLR/AuC, Application Servers etc.

(b) Authorization of user equipment.

(c) Storage of access and mobility data and session management data needed by NF consumers to implement application logic.

(d) 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.

(e) 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.

(f) 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.

(g) 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. Monitoring of various events configured via UDM

(h) Nudr_DataRepository services:

1. Service operations like Create, Delete, Update, Notify, Subscribe, unsubscribe;
2. HTTP GET and HTTP POST method for Query and subscribe operation; and
3. OAuth2/ other applicable protocols to grant services for NF consumers.

(i) 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
3. An overload threshold value shall be set. Once the UDR loading reaches the threshold value, the system shall generate alarms before service impact.

(j) 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.

(k) N+K redundancy at data service level.

(l) Nudr proxy between UDR instances secured through mTLS.

(m)Following NRF services:

1. NFStatusSubscribe, NFStatusUnsubscribe, NFRegister;

2. NFUpdate, NFDeregister, NFListRetrieval, NFProfileRetrieval;

3. Nnrf_AccessToken service, Heat Beat Service mechanism;

4. Nnrf_NFManagement service; and

5. Nnrf_NFDiscovery service.

(n) Ability to identify and remove inconsistent data

(o) Migration of subscribers from multiple 2G/3G/4G repository (backend of HLR/HSS) systems to a single UDR.

(p) Storage and retrieval of policy data on behalf of the PCF.

(q) Storage and retrieval of structured data for exposure, e.g. application data including Packet Flow Descriptions

(r) Being reachable only by NF service consumers within the same PLMN/network via the Nudr interface.

3.7. NRF (Network Repository Function)

NRF provides a single record of all network functions (NF) available in a given PLMN, together with the profile of each and the services they support.

3.7.1. NRF functional requirements:

3.7.1.1. NRF shall be connected with other 3GPP network elements using standard Service Based Interface (SBI)

(a) AMF;
(b) SMF
(c) UDM;
(d) AUSF;
(e) NEF;
(f) PCF;
(g) SMSF;
(h) NSSF; and
(i) UPF

3.7.1.2. The NRF shall support:

(a) Following services:

1. Nnrf_NFManagement service;
2. Nnrf_NFDiscovery service;
3. Nnrf_AccessToken service;
4. Nnrf_Bootstrapping service;
5. NFRegister service;
6. NFUpdate service;
7. NF Heart-Beat service;
8. NFDeregister service;
9. NFStatusSubscribe service;
10. NFStatusNotify service;
11. NFStatusUnSubscribe service;
12. NFListRetrieval service; and

13. NFProfileRetrieval service.

(b) Subscription and notification to other NFs regarding the registration in NRF of new NF instances of a given type;

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

(d) 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.

(e) 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.

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

(g) 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.

(h) Returning "404 Not Found" status code with the ProblemDetails IE providing details of the error if the NF Instance identified by the "nfInstanceID", is not found in the list of registered NF Instances in the NRF's database in Delete request.

(i) 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.

(j) 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.

(k) 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.

(l) 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.

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

(n) Geo-redundancy or disaster recovery architecture without any data loss or service outage.

(o) P-CSCF discovery as a specialized case of AF discovery by the SMF.

3.7.1.3. NRF may support:

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

(b) Data structures and URI query parameters as defined in clause 6.1.3.2.3.1 of 3GPP TS 29.510.

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

(d) 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.

(e) Blocking of Register operation to be invoked from an NRF in a different PLMN

3.8. PCF (Policy Control Function)

Support of 5G QoS policy and charging control functions and the related 5G signalling interfaces. The 3GPP interfaces, such as N7, N15, N28, N36, and Rx, define these interfaces for the 5G PCF.

3.8.1. PCF functional requirements:

3.8.1.1. The PCF shall support:

(a) Interactions with the access and mobility policy enforcement in the AMF, through service-based interfaces;

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

(c) Handling of UE Context Establishment request as a part of UE Registration;

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

(e) Session management related functionality of Policy and charging control for a service data flow;

(f) Session management related functionality of PDU Session related policy control.

(g) 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.

(h) 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.

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

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

(k) Control of QoS for the packet traffic of the PDU Session.

(l) Mechanism to initiate QoS Flow establishment and modification as part of the QoS control; and

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

(n) 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 (PDN) the user is accessing, if present.

(o) 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.

3.8.1.2. The PCF may modify:

(a) the authorized Session AMBR at any time during the lifetime of the PDU session and provision it to the SMF; and

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

3.8.1.3. The PCF may reject the request received from the AF when the service information is not consistent with either the related subscription information or the operator defined policy rules and as a result the PCF shall indicate that this service information is not covered by the subscription information or by operator defined policy rules and may indicate, in the response to the AF, the service information that can be accepted by the PCF (e.g. the acceptable bandwidth).

3.8.1.4. The PCF may be the capability to take a PCC rule into service, and out of service, at a specific time of day

3.8.1.5. The PCF may support selective Blocking of RCS Services based on PLMN, TAI and Postpaid/Prepaid Subscription.

3.8.1.6. The PCF may support setting and sending applicable thresholds to the SMF for monitoring, in case the PCF uses usage monitoring for making dynamic policy decisions.

3.9. NEF (Network Exposure Function)

This function provides a means to securely expose the services and capabilities provided by 3GPP network functions.

3.9.1. NEF functional requirements:

3.9.1.1 NEF shall be connected with other 3GPP network elements using standard Service based interface

(a) NRF;

(b) BSF;

(c) PCF, N30; and

(d) AF, N33

3.9.1.2 NEF may be connected with other 3GPP network elements using standard Service based interface

(a) UDR, N37;

3.9.1.3 The NEF shall support following services:

(a) Service-based interface Nnef;

(b) Non-roaming architecture;

(c) Subscribe service for Nnef_EventExposure Service;

(d) Unsubscribe Service Operation of Nnef_EventExposure Service;

(e) Notify Service Operation of Nnef_EventExposure Service; and

(f) Monitoring with the Nnef_EventExposure Service.

3.9.1.3. The NEF shall support:

(a) Masking of network and user sensitive information to external AF's according to the network policy.

(b) 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.

(c) Translatation of information exchanged with the AF and information exchanged with the internal network function.

(d) Small-scale deployments, e.g. for dedicated enterprise solutions, and/or small distributed edge cloud deployments.

(e) 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.

(f) CAPIF functionality for API-invoker/exposure-function registration.

3.9.1.4. The NEF may support:

(a) Procedure for resource management of Background Data Transfer (BDT). Also NEF shall support Resource Management of BDT API for background data transfer.

(b) Nnef_TrafficInfluence service, Nnef_BDTPNegotiation service, Nnef_ChargeableParty service, Nnef_AFsessionWithQoS service, NF_management operations with NRF, exposure of bulk subscription.

3.9.1.5. NEF shall translate information exchanged with the AF and with internal Network function. NEF architecture shall integrate with the different elements of the 5G core. The own/partnership/normalized description, third parties and Open Source dependencies shall be indicated.

3.10. NSSF (Network Slicing Selection Function)

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.

3.10.1. NSSF functional requirements:

3.10.1.1. NSSF shall be connected with other 3GPP network elements using Standard Service based Interface

(a) NRF;

(b) AMF;

(c) SCP; and

(d) EMS

3.10.1.2. NSSF may be connected with other 3GPP network elements using Standard Service based Interface

(a) SEPP;

3.10.1.3. The NSSF shall support:

(a) Determination of the Allowed NSSAI.

(b) Determination of the AMF Set to serve the UE.

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

(d) selection of service based on slice such as eMBB, URLLC, mIoT.

(e) Roaming architecture for Home Routed traffic.

(f) Selection of same AMF for different set of slices.

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

(h) Provision of configured slice information for the PLMN when requested with “default configured S-NSSAI “indication;

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

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

(k) Nnssf_NSSelection service for Network Slice selection in both the Serving PLMN and the HPLMN. Example AMF, V-NSSF, SMF.

(l) Provision of the AMF set or the list of candidate AMF to be used to serve the UE by querying the NRF

3.10.1.4. The NSSF may support following services:

(a) NFStatusSubscribe service; and

(b) NFProfileRetrieval service

(c) NFRegister service;

(d) NFDeregister service; and

(e) NFStatusNotify service.

3.10.1.5. NSSF may have capability to provide bulk provisioning over all exposed interfaces. It shall provide Real time subscriber data synchronization.

3.11. BSF (Binding Support Function)

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

3.11.1. BSF functional requirements:

3.11.1.1. The BSF shall comply with the applicable requirements, procedures, service operations, interfaces and functionalities as specified in the relevant 3GPP standards, as applicable to the BSF and limited to the functionalities supported by the BSF.

3.11.1.2. The BSF shall support:

(a) Registration of BSF profile with NRF.

(b) heartbeat procedure periodically with NRF to update NF status. This heartbeat message shall also include BSF load information.

(c) Discovery of BSF via Nnrf_Discovery API by the NF Consumers (NEF or AF) .

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

(e) Binding between PCF and NEF or AF.

(f) Binding lookup on receipt of Diameter (Rx) message from AF and route it to appropriate PCF based on binding information.

(g) DIAMETER (Rx) Proxy or Redirect request based on UE's IP address.

(h) Return an appropriate error response when no PCF binding exists for a discovery request.

3.11.2. BSF QoS requirements

3.11.2.1. The BSF shall support:

(a) Use of Nbsf_Management_Register, Nbsf_Management_Deregister and Nbsf_Management_Update service operations by PCF; and

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

(c) 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.

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

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

3.12. CHF (Charging Function)

CHF allows charging services to be offered to authorized network functions. A converged online and offline charging will also be supported.

3.12.1. CHF functional requirements

3.12.1.1. The CHF shall support:

(a) 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. Video, HTTP, WiFi
6. URL based charging

(b) 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
4. CDRs generation

(c) N40 interface with the SMF for Data Connectivity Charging, which includes:

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

(d) Time based, volume based and event based charging and any such combination.

(e) 3GPP specified services;

(f) Consumption of services exposed by the NRF

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

(h) Spending Limit Control Service of the Nchf Service according to 3GPP TS 32.290 and 3GPP TS 29.504 (Optional);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;

(i) 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;

(j) Upgradeability to 3GPP Rel-16 functionality and also backward compatibility;

(k) All mandatory fields for CDR in 3GPP TS 32.255;

(l) 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);

(m) Charging of roaming traffic;

(n) Below interface function from CHF perspective

1. Support Interface with AMF/SGSN/MME/SMF/UPF/SPGW; and
2. CHF to Register/update/deregister towards NRF.

(o) Converged online and offline charging triggered from Session Management Function (SMF), CHF shall also support following notification requirements –

1. Nchf_ConvergedCharging_Create/ Update/ Delete /Notify
2. Nchf_SpendingLimitControl_Subscribe/Unsubscribe/Notify

(p) Different charging between 4G and 5G.

3.12.1.2. CHF may support charging of 5G sessions in case of Session and Service Continuity mode, as defined in 3GPP TS 32.255;

3.12.2. CHF QoS requirements.

3.12.2.1. CHF shall support:

(a) 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);

(b) 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;

(c) Integration of 4G Charging and 5G charging;

(d) Charging of services based on network slice, as well as charging as per network slice management; and

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

3.13. SMSF (Short Message Service Function)

SMSF is a system required for the provision of SMS over NAS through AMF.

3.13.1. SMSF functional requirements:

3.13.1.1. The SMSF shall support:

(a) Standard Namf interface function.

(b) Standard Nsmsf interface function.

(c) Standard Nudm interface function.

(d) Nnrf_NFManagement Service API.

(e) Nnrf_NFDiscovery Service API.

(f) OAuth2.0 Authorization Service API.

(g) Informing NRF of load, priority and capacity.

(h) Generating SMS related CDR.

(i) SMS over NAS.

(j) Call barring based on information received from UDM.

(k) Local configuration for node selection in the event if NRF is unreachable.

(l) SMS management subscription data checking and conducting SMS delivery accordingly, which includes ODB checking and if MT SMS is authorized.

(m) Error handling & rerouting to alternate NF or reject the request in case of error.

(n) Configuring heartbeat interval timer.

3.13.1.2. 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.

3.14.1. The NWDAF shall allow NF consumers to subscribe to and unsubscribe from periodic notification and/or notification when a threshold is exceeded.

3.14.2. The NWDAF shall support one or more of the following functionalities:

(a) Identifier of network slice instance; and

(b) load level information for that network slice instance.

(c) Support data collection from NFs and AFs;

(d) Support data collection from OAM;

(e) NWDAF service registration and metadata exposure to NFs and AFs;

(f) Support analytics information provisioning to NFs and AFs;

(g) Support Machine Learning (ML) model training and provisioning to NWDAFs (containing Analytics logical function).

(h) Nnwdaf_AnalyticsInfo and Nnwdaf_AnalyticsSubscription services to provide analytics information to consumer NFs.

(i) Nnwdaf_MLModelProvision service where the NWDAF instance provides Machine-Learning models to other NWDAF instances

(j) Register its analytics-exposure capability with the NRF for discovery.

(k) Nnwdaf_MLModelInfo for exchange of trained Machine-Learning model metadata between NWDAF instances.

3.15. DCCF (Data Collection Coordination Function)

The DCCF coordinates the collection of data required for analytics and network optimization. It manages data collection requests and interactions between data producers and analytics consumers.

3.15.1. The DCCF shall support:

a) Coordination of data collection requests from NWDAF and other consumer NFs

towards data source NFs.

b) Subscription to data delivery from data source NFs when the requested data is not already being collected.
c) Collection of data from any 5GC NF, OAM or NWDAF and delivery of the collected data to requesting consumer NFs or NWDAF instances.
d) Direct delivery of collected data to consumer NFs or NWDAF, or indirect delivery through the Messaging Framework and MFAF.
e) Coordination of historical data collection and retrieval for NWDAF analytics generation.
f) Registration and management of data collection profiles.
g) Storage of collected data in ADRF when requested by a consumer NF or configured by the operator.
h) Registration, update and deregistration of collected data context information through Ndccf_ContextManagement services.
i) Authorization and policy enforcement for access to collected data and analytics information.

3.15.2. The DCCF may support:

a) Messaging Framework and MFAF for data collection and delivery instead of direct collection from NFs.
b) Aggregation of identical data requests from multiple consumers to reduce signaling overhead and duplicate data collection.

3.16. ADRF (Analytics Data Repository Function)

The ADRF stores analytics information generated or consumed by analytics-related network functions. It provides persistent storage and retrieval of analytics data for authorized consumers.

3.16.1. The ADRF shall support:

a) Nadrf service for storage and retrieval of analytics and collected network data by authorized 5G Core Network Functions.
b) Storage, retrieval, and deletion of analytics and collected network data received directly from authorized Network Functions or indirectly through DCCF, NWDAF, and MFAF
c) Subscription-based storage and retrieval of analytics and collected network data, including notification and subscription management.
d) Authorization mechanisms to ensure that only authorized Network Functions can access ADRF services and stored information.

3.16.2. The ADRF may support:

a) Selection of data from specific data sources or Network Functions (NFs) for archiving based on operator configuration or information obtained from the Network Repository Function (NRF).
b) Reception of analytics and collected network data from multiple sources, including the Data Collection Coordination Function (DCCF) and the Messaging Framework.
c) Detection and avoidance of duplicate storage of analytics and collected network data.
d) Provision of references or fetch instructions for efficient retrieval of large datasets by authorized Network Functions (NFs).

3.17. MFAF (Messaging Framework Adaptor Function)

The MFAF provides adaptation between the 5G Core and messaging service frameworks for messaging-related services.

3.17.1. The MFAF shall support:

a) Retrieval of analytics data, including historical analytics, from the Network Data Analytics Function (NWDAF).
a) Configuration and management of analytics data processing, mapping, and delivery.
b) Delivery of analytics data to authorized Network Functions through notification and on-demand retrieval mechanisms.
c) Nmfaf_3daDataManagement service for data-notification distribution to consumer NFs

3.17.2. The MFAF may support:

a) Collection and delivery of data between Network Functions (NFs) and the Network Data Analytics Function (NWDAF) through the Messaging Framework.
b) Collection and delivery of analytics between the Network Data Analytics Function (NWDAF) and consumer Network Functions (NFs) through the Messaging Framework.
c) Storage of data in the Analytics Data Repository Function (ADRF)..
d) Protocol translation between 3GPP-defined interfaces using Messaging Framework adaptors.

3.18. 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.

3.18.1. The Security Edge Protection Proxy (SEPP) is a non-transparent proxy and shall support:

(a) 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.

(b) Topology hiding. The SEPP applies the above 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 interPLMN signalling between the SEPPs may pass via IPX entities.

(c) Perform mutual authentication and key management with the peer SEPP for N32-c/N32-f establishment

3.19. SCP (Service Communication Proxy)

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

3.19.1. The SCP shall support:

(a) HTTP/2 connection management between the HTTP client, SCP, and HTTP server.
(b) Establishing or reusing a connection to the next-hop SCP when forwarding requests.
(c) Modification of HTTP/2 pseudo-headers when forwarding requests to the target NF
(d) Selection of the target NF service instance using the discovery factors when required.
(e) Routing requests to the selected NF service instance of the target NF service producer.

3.19.2. SCP may support Communication security,load balancing, monitoring, overload control etc.

3.19.3. The Service Communication Proxy (SCP) includes one or more of the following functionalities. Some or all of the SCP functionalities may be supported in a single instance of an SCP:

(f) Model D Indirect Communication.
(g) Delegated Discovery.
(h) Message forwarding and routing to destination NF/NF service.
(i) Message forwarding and routing to a next hop SCP.
(j) Retry handling and priority-based load balancing across NF service producers.

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

3.20. N3IWF (Non-3GPP Interworking Function)

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

3.20.1. The N3IWF shall support:

a) 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.

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

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

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

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

f) 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.
4. Supporting AMF selection.

3.21. LMF (Location Management Function)

The LMF provides positioning services and calculates the geographical location of a UE using positioning measurements and assistance data. It supports various positioning methods and interacts with the AMF, (R)AN, GMLC, and other network functions

3.21.1. LMF Functional Requirements:

3.21.1.1. LMF shall support;

a) Co-ordination and scheduling of resources required for the location of a UE that is registered with or accessing 5GCN

b) Calculation, verification or inclusion of the final UE location and any velocity estimate.

c) Estimation of the achieved positioning accuracy, if available.

d) Receipt of location requests for a target UE from the serving AMF using the Nlmf interface.

e) Interaction with the UE to exchange location information applicable to UE-assisted and UE-based positioning methods.

f) Interaction with the NG-RAN to obtain location information.

g) Determination of the positioning result in geographical coordinates as specified in 3GPP TS 23.032.

h) Provision of the Nlmf_Location service to enable Network Functions to request location determination for a target UE

i) Provision of UE location information to the NF Service Consumer using the Determine Location service operation

j) Return of the determined location information, including the geographical area, positioning method upon successful location determination.

k) Broadcast and unicast positioning assistance-data delivery to the UE via the AMF/NG-RAN.

3.21.1.2. LMF may support;

a) Periodic or triggered location requests received from the serving AMF for a target UE, report the UE location estimates directly to the GMLC, and support cancellation of those periodic or triggered location requests.

b) Change of a serving LMF for periodic or triggered location reporting for a target UE.

c) Inclusion of positioning method information and age of the location

estimate in the location response.

d) Inclusion of altitude information in the positioning result, where available.

e) Inclusion of GNSS positioning information in the location response, where available.

l) Interaction with N3IWF or TNAN to obtain location information.

3.22. GMLC (Gateway Mobile Location Centre)

The GMLC acts as the gateway for external and internal location service requests. It authorizes, coordinates, and routes positioning requests to the appropriate network functions to obtain UE location information.

3.22.1. The GMLC shall support:

a) Authorization of an external LCS Client before processing a location request.
b) Ngmlc_Location Service
c) The Ngmlc_Location API
d) 3gpp-Sbi-Message-Priority HTTP custom header
e) Sending an HTTP POST request to the callback URI of the NF consumer, with the response body containing a LocUpdateNotification object

3.22.2. The GMLC may support:

a) Determination of the serving AMF for a target UE when more than one serving AMF is available.
b) Determination of whether to attempt a second location request for a target UE through a different AMF when the location information returned by the first AMF does not meet the required QoS and more than one serving AMF is available.
c) Retrieval of routing information and/or target UE privacy information from the UDM via the Nudm interface.
d) Support for location requests from an external LCS Client or NEF for 5GC-MT-LR and deferred 5GC-MT-LR for periodic, triggered and UE available location events.
e) Forwarding of location requests for a roaming UE to a VGMLC or serving AMF in the VPLMN based on deployment configurations.
f) Reception of event reports from a VGMLC or LMF for deferred 5GC-MT-LR and returning them to an external LCS Client or NEF.

g) Cancellation of periodic or triggered location requests.
h) Reception of location information from a VGMLC for a 5GC-MO-LR and forwarding it to an LCS Client or an AF via the NEF, if requested by the UE.
i) Reception of location requests from an HGMLC for a roaming UE and forwarding them to the serving AMF.
j) Reception of event reports from an LMF for deferred 5GC-MT-LR for a roaming UE and forwarding them to the HGMLC.
k) Reception of location information from an AMF for a 5GC-MO-LR and forwarding it to the HGMLC.
l) Rejection of an LCS request from an LCS Client when the number of target UEs exceeds the maximum target UE number supported for that client.
m) Allocation of a reference number for each location request received from an external LCS Client or NEF for LDR.
n) Assignment of a pseudonym when a pseudonym indicator is received in the service request and transfer of the pseudonym to the external LCS Client.
o) Interfacing with a legacy GMLC for interworking with 4G positioning deployments if applicable
p) Verification of the target UE privacy before forwarding a location request.
q) Forwarding of a location request to the serving AMF via the Namf interface or to a GMLC in another PLMN via the Ngmlc interface for a roaming UE.

3.23. UDSF (Unstructured Data Storage Function)

The UDSF stores and retrieves unstructured data on behalf of authorized network functions. It enables data persistence and sharing without defining the data structure or format.

3.23.1. The UDSF shall support:

a) Storage and retrieval of unstructured data for 5GS Network Functions.
b) Query operations for stored unstructured data.
c) Creation, update and deletion of records, blocks, metadata, metadata schema, subscription notifications and bulk records, as applicable.
d) Notification procedures for record expiry, data change and subscription expiry.
e) Subscription and unsubscription procedures for data change notifications.
f) Timer expiry notification to NF service consumers.
g) Storage and retrieval APIs independent of the data model used by the consuming NF.

3.23.2. The UDSF may support:

a) Sharing of a common UDSF among multiple Network Functions within a PLMN based on operator configuration
b) Deployment of dedicated UDSF instances for individual Network Functions based on operator configuration
c) Notification of NF service consumers upon record expiry based on record expiry details.
d) Meta Schema feature for optimization of UDSF data storage and search access.

3.24. NSACF (Network Slice Admission Control Function)

The NSACF performs admission control for network slice access based on operator policies and slice resource availability. It assists in determining whether a UE can be admitted to a requested network slice.

3.24.1. The NSACF shall support:

a) Monitoring and controlling the number of registered UEs and active PDU Sessions for network slices subject to Network Slice Admission Control (NSAC).
b) Configuration of the maximum number of registered UEs and active PDU Sessions permitted per S-NSSAI.
c) Configuration of the applicable access type(s) for each S-NSSAI, including 3GPP Access, Non-3GPP Access, or both.
d) Maintenance of the current count of UEs registered for each network slice.
e) Maintenance of a list of UE IDs registered with network slices subject to NSAC.
f) Updating the current number of PDU Sessions based on the applicable access type for NSAC.
g) Provision of event-based notifications and reports on the number of registered UEs and active PDU Sessions to subscribed consumer Network Functions (NFs).

3.24.2. The NSACF may support:

a) Support for one or more S-NSSAIs.
b) Deployment on a service area basis as a single NSACF instance or an NSACF Set when the network is configured with multiple service areas.
c) Consideration of the Access Type when increasing or decreasing the number of UEs per network slice by storing the UE ID together with one or more associated Access Types.

d) Provision of Network Slice status notifications and reports to consumer Network Functions (NFs), such as the AF through the NEF.

3.25. NSSAAF (Network Slice Specific Authentication and Authorization Function)

The NSSAAF performs slice-specific authentication and authorization for UEs accessing particular network slices. It enables additional security procedures beyond primary network authentication when required.

3.25.1. The NSSAAF shall support:

a) Slice-specific authentication and authorization with the AAA Server (AAA-S).
b) Handling of network slice-specific authentication requests received from the serving AMF.
c) AAA Server (AAA-S)-initiated network slice-specific re-authentication, re-authorization, and authorization revocation.
d) Translation between Service-Based Interface (SBI) messages and AAA protocols for communication with the AMF, AUSF, and AAA Server/Proxy (AAA-S/AAA-P).
e) Access to Standalone Non-Public Networks (SNPNs) using credentials from the Credentials Holder through the AAA Server.

3.25.2. The NSSAAF may support:

a) Contacting the AAA Server (AAA-S) through a AAA Proxy (AAA-P) when the AAA-S belongs to a third party.
b) Access to SNPN using credentials from Default Credentials Server using AAA Server (AAA-S).
c) Discovery through the NRF unless NSSAAF information is available by other means, e.g. locally configured on the NF consumer.

3.26. AAnF (AKMA Anchor Function)

The AANF supports AKMA (Authentication and Key Management for Applications) by managing AKMA-related context and key information. It enables secure authentication and key distribution for AKMA-enabled applications.

3.26.1. The AAnF shall support:

a) Storage and update of the latest AKMA context received from the AUSF, including

replacement of obsolete AKMA information.

b) Provision of confidentiality, integrity, and replay protection on the Service-Based Architecture (SBA) interfaces with the AUSF, AF, and NEF.
c) Protection of transported data exchanged with the AF and NEF against unauthorized disclosure, modification, and replay attacks.
d) Act as the anchor function that derives the AKMA Application Key (K_AF) from the AKMA Anchor Key (K_AKMA) received from AUSF
e) Maintain a UE's AKMA context and provide the K_AF to an Application Function upon request via Naanf_AKMA service

3.27. UCMF (UE Radio Capability Management Function)

The UCMF manages UE radio capability information within the 5G Core network. It stores, processes, and provides UE radio capability data to authorized network functions to improve network operation and signaling efficiency.

3.27.1. The UCMF shall support:

a) Resolution of a UE Radio Capability ID (either Manufacturer-assigned or PLMN-assigned) into the corresponding UE Radio Access Capability Information and the corresponding UE Radio Capability for Paging.
b) Provision of a PLMN-assigned UE Radio Capability ID for a specific UE Radio Access Capability Information.
c) Subscription and Unsubscriotion for notifications of UCMF dictionary entries.
d) Assignment of a PLMN-assigned UE Radio Capability ID by providing UE Radio Access Capability Information.
e) Verifying the uniqueness and consistency of the UE Radio Capability ID across manufacturer-assigned and PLMN-assigned ID spaces

3.28. MBSF (Multicast Broadcast Service Function)

The MBSF provides service-layer support for multicast and broadcast services in the 5G system. It coordinates service-related procedures and interacts with the MB-SMF for MBS session management.

3.28.1. The MBSF shall support:

a) Reception of multicast/broadcast service requests from the AF, either directly or through the NEF.
b) Interaction with the MB-SMF for creation, modification, activation, deactivation and

release of MBS sessions.

c) Determination of the QoS requirements for MBS sessions, including support for service-specific requirements such as Forward Error Correction (FEC), and provision of the determined QoS requirements to the MB-SMF.
d) Delivery of service announcement information to UEs for multicast and broadcast services.
e) Interaction with the MBSTF for user plane ingress resource allocation and content delivery management.
f) Support for MBS security functions together with MBSTF for protection of MBS signalling and user data.
g) Reception of notifications related to MBS session events, such as session release due to TMGI expiry and broadcast delivery status.
h) Service layer interworking between 5G MBS and LTE eMBMS/MBMS services.

3.28.2. The MBSF may support:

a) Selection and control of MBSTF for content ingestion and transport resource management.

3.29. MB-SMF (Multicast Broadcast Session Management Function)

The MB-SMF manages multicast and broadcast PDU sessions within the 5G system. It establishes, modifies, and releases multicast/broadcast session resources and coordinates with other network functions.

3.29.1. The MB-SMF shall support:

a) Multicast and Broadcast MBS Session Management, including QoS control for MBS sessions.
b) Configuration of the MB-UPF for multicast and broadcast data transport based on policy rules received from PCF or local policy.
c) Allocation and de-allocation of TMGI (Temporary Mobile Group Identity) for MBS sessions.
d) Interaction with NG-RAN via AMF to control data transport using 5GC Shared MBS Traffic Delivery Method for Broadcast MBS sessions.
e) Interaction with SMF to provide MBS Session Context information for Multicast MBS sessions.
f) Interaction with NG-RAN via AMF to establish data transmission resources between MB-UPF and NG-RAN for 5GC Shared MBS Traffic Delivery for multicast services.
g) Control of MB-UPF for multicast data transport using 5GC Individual MBS Traffic

Delivery Method.

h) Support of multicast session Activation and Deactivation procedures triggered by AF requests or MB-UPF notifications.
i) Registration of MB-SMF capabilities such as S-NSSAI, DNN, TMGI range and service area information in NRF for MB-SMF discovery and selection.

3.29.2. The MB-SMF may support:

a) Selection of appropriate MB-UPF and reservation of ingress transport resources for MBS distribution sessions.
b) Reception of updated policy rules from the PCF and application of the rules for MBS session management and QoS updates.
c) Event subscription and notification for multicast session state changes, QoS changes, service area changes, TMGI expiry, and broadcast delivery status.

3.30. TSCTSF (Time Sensitive Communication Time Synchronization Function) (Optional)
The TSCTSF provides time synchronization support for Time Sensitive Communication (TSC) services. It distributes synchronization information required to achieve precise timing for TSC-enabled applications.
3.30.1. The TSCTSF shall support:

a) Operation as the central time synchronization entity within the 5G System for Time Sensitive Communication (TSC) services..
b) Provision of time synchronization within the 5G System for Time Sensitive Communication (TSC) services.
c) Provision of time synchronization information between the 5G System, User Equipment (UE), and external Time Sensitive Networking (TSN) networks..
d) Coordination of synchronization-related policies and Quality of Service (QoS) requirements for Time Sensitive Communication (TSC) services.
e) Management of synchronization domains, including Grandmaster Clock selection.
f) Fulfilment of synchronization accuracy requirements for Time Sensitive Communication (TSC) services.

3.30.2. The TSCTSF may support:
a) Integration with external IEEE Time Sensitive Networking (TSN) Centralized Network Configuration (CNC) entities for network-wide scheduling and synchronization management.

b) Support for multiple synchronization domains and multiple grandmaster clocks.
c) Distribution of synchronization status and timing quality information to applications and network functions.

3.31. 5G-EIR (5G-Equipment Identity Register)

The 5G-EIR stores equipment identity information and determines whether a UE is allowed to access the network based on its equipment identity. It supports equipment identity verification using the PEI/IMEI.

3.31.1. The 5G-EIR shall support:

a) Checking the Permanent Equipment Identifier (PEI) and determining whether the PEI is in the blacklist or not.
b) Processing of equipment identity check requests and returning the corresponding equipment status.
c) Provision of equipment status values, including Whitelisted, Blacklisted, and Greylisted.

3.31.2. The 5G-EIR may support:

a) Inclusion of SUPI in the equipment identity check request.
b) Inclusion of GPSI in the equipment identity check request.
c) Performance of ME identity check during procedures establishing a signalling connection with the UE.
d) Interworking with the legacy EIR used for 4G equipment-identity checks

3.32. TNGF (Trusted Non-3GPP Gateway Function)

The TNGF provides trusted non-3GPP access to the 5G Core network. It supports secure connectivity and mobility for UEs accessing the network through trusted non-3GPP access technologies.

3.32.1. The TNGF shall support:

a) Connectivity of the UE to the 5G Core Network through trusted non-3GPP access technologies, including trusted WLAN and other trusted non-3GPP access networks supported by the 5G System.
b) Secure connectivity between the UE and the 5G Core over trusted non-3GPP access, including establishment, maintenance, modification, rekeying, liveness verification,

and release of IKEv2 and IPsec Security Associations.

c) UE registration, transport of NAS signalling, and control plane communication over trusted non-3GPP access.
d) Transport of user plane traffic over trusted non-3GPP access, including appropriate encapsulation and forwarding mechanisms.
e) Quality of Service (QoS) management for trusted non-3GPP access, including QoS differentiation, mapping of QoS Flows to access network resources, and reservation of QoS resources.
f) Management of IPsec Child Security Associations in relation to PDU Sessions and QoS Flows, including determination, establishment, selection, and maintenance of Security Associations for user plane traffic.

3.32.2. The TNGF may support:

a) Mobility and Multihoming Protocol (MOBIKE) for IKEv2.
b) Additional QoS information associated with IPsec Child SAs.
c) Access to PLMN services via SNPN and SNPN services via PLMN using dedicated QoS profiles.
d) Reservation of non-3GPP access resources based on operator policies and local configuration.

3.33. TWIF (Trusted WLAN Interworking Function)

The TWIF enables trusted WLAN access to the 5G Core network. It provides interworking functions between trusted WLAN networks and the 5G Core while supporting secure UE connectivity.

3.33.1. The TWIF shall support:

a) Connectivity of UE to the 5GC through trusted WLAN access networks.
b) Authentication procedures for trusted non-3GPP access as specified for trusted WLAN access.
c) Secure transport of NAS signalling between the UE and AMF over trusted WLAN access.
d) UE registration over trusted WLAN access.
e) PDU Session establishment and release procedures for UEs connected through trusted WLAN access.
f) QoS handling and mapping of QoS Flows to WLAN bearer resources.
g) Mobility between 3GPP access and trusted WLAN access.

h) Mobility between trusted WLAN access and other non-3GPP accesses where applicable.
i) User plane traffic forwarding between WLAN access and UPF.
j) NAS message transport over trusted WLAN access.
k) Security key derivation and management using KTWIF.
l) Protection of signalling and user plane traffic over trusted WLAN access.
m) Trusted WLAN access procedures defined for the 5GS architecture.

3.33.2. The TWIF may support:

a) Simultaneous access using both 3GPP and trusted WLAN access networks.
b) Policy-based traffic steering between WLAN and 3GPP accesses.
c) WLAN access optimization features defined by operator policies.
d) Support for network slicing over trusted WLAN access.

3.34. Application Function (AF)

The Application Function (AF) provides application-related information to the 5G Core network to influence network behavior according to application requirements.

3.34.1. The AF shall support:

a) Interaction with the Policy Control Function (PCF) to provide application information and policy control requirements.
b) Provision of application requirements to influence Quality of Service (QoS) and User Plane traffic routing.
c) Interaction with the 5G Core through standardized network exposure mechanisms, including the Network Exposure Function (NEF), where applicable.
d) Provision of application information to enable edge computing services, where applicable.

3.34.2. The AF may support:

a) Interaction with the Policy Control Function (PCF) either directly or through the Network Exposure Function (NEF), subject to operator policy.
b) Provision of application information for local traffic routing and edge application deployment.
c) Application-triggered policy updates during the lifetime of a PDU Session.

Chapter 4

1. 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.

1.1. Management Functions

The following management functions shall be carried out through the corresponding OMCs:

1.1.1. Configuration management

1.1.2. Fault report and alarm handling

1.1.3. Performance supervision/management

1.1.4. Storage of system software and data

1.1.5. Security management

1.2. OMC database

1.2.1. The OMC shall use the relational/object-oriented database to store and hold the necessary information for the parameters used in the OMC.

1.2.2. The OMC database shall include configuration data, maintenance data, fault data and performance / QoS data.

1.2.3. The database in the OMC shall reside in a disk with mirroring capability.

1.2.4. 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.

1.2.5. Provision shall be available for collection of statistical information relating to events in the network. Collection frequency shall be configurable

1.2.6. 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:

1.2.6.1. Network elements

1.2.6.2. Severity class

1.2.6.3. Event type

1.3. OMC Generic Features

1.3.1. OMC software – UNIX/LINUX/Windows System Platform

1.3.2. It shall optionally support interface like CORBA / TCP / IP / CMIP / SNMP/ REST / HTTP etc., to enable it to work with a remote NMS.

1.3.3. Support Ethernet connectivity with remote network elements.

1.3.4. Graphical User Interface (GUI). [Alternate text: Management through Element Management System]

1.3.5. On-Line Help.

1.3.6. Consistency Checks.

1.3.7. Configuration Change/Event Log.

1.3.8. Object Alarm Status Management / Display.

1.3.9. Collection of PM counters.

1.3.10. Limited Access Restriction by User.

1.3.11. Access Restriction by Function and by Operation.

Chapter 5

2. Non-functional Requirements

2.1. The Network functions shall support:

(a) Command Line Interface (CLI).

(b) Secure File Transfer Protocol like SFTP and SSH for login

(c) Micro service-based architecture.

(d) Different redundancy model (i.e. Active-Active, Active-Standby, N-Way Active) for each type of microservices

(e) Capability to store and retrieve all security related information. Information shall range from security access levels to login times by user id, to password aging data.

(f) Having their own self-diagnostic functionality to provide their health information.

(g) Modularity and have a distributed architecture.

(h) Implementation on carrier class server/cloud.

(i) Software executable (patch) upgrade with / without configuration migration.

(j) virtualised solution on generic COTS hardware or shall support Cloud Integration.

2.2. The Network functions shall allow the independent scaling of the microservices

2.3. 5G Core shall guarantee carrier-grade 99.999% system availability and avoid any Single Point of Failure.

2.4. Applications shall support different deployment options e.g. Metal server or container infrastructure

2.5. The System shall provide the Trace Analysing tool or a mechanism for providing all successful and Failure call trace for subscriber level.

2.6. No single failure of any module within the System, Network Element, shall lead to total disruption of service of that NE. Such failure shall also lead to minimum possible degradation of performance.

2.7. The Network function may have the capability of scale in/ scale out when certain KPI thresholds are reached such as CPU, Average Memory, and Load etc. Also, may support life cycle management procedures such as VNF/CNF instantiation & VNF/CNF termination manually and automatically

2.8. The System shall be able to create, modify and delete commands from command classes. Also, System shall support definition of access privileges like read-only/write/import/export for groups or roles.

2.9. VNF/CNF shall maintain the feature parity with native solution.

2.10. VNF/CNF shall include application level fault tolerance on compute, storage and network.

2.11. VNF/CNF shall provide and maintain Telecom Grade KPI.

2.12. VNF/CNF shall be agnostic to all 3GPP access types.

2.13. For security purpose, all components of Virtualized System, e.g. MANO, VNF/CNF depository etc. shall be hosted in India only.

2.14. VNF/CNF shall meet availability requirements as envisaged in this GR.

Chapter 6

3. Generic Common Requirements

3.1. Operation & Maintenance

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

3.1.1. The NFs shall provide a flexible & secure management interface for configuration, fault management and performance management.

3.1.2. The NFs shall include an O&M interface for debugging and troubleshooting.

3.1.3. NFs shall support at least one of the following interfaces towards EMS

3.1.3.1. SNMP (Is it required for 5G?)

3.1.3.2. REST

3.1.3.3. HTTPS

3.1.4. For performance management, the node shall generate various performance counters and provide mechanism to transfer the same to external entity for further analysis.

3.1.5. Fault Report and Alarm Handling

3.1.5.1. 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.

3.1.5.2. Fault Management system shall have the ability to detect and mitigate or recover from faults.

3.1.5.3. Fault Detection and Isolation

3.1.5.4. 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

3.1.5.4.1. Alarm type

3.1.5.4.2. The probable cause

3.1.5.4.3. The specific problem

3.1.5.4.4. The perceived severity

3.1.5.4.5. Network Element ID

3.1.5.4.6. Network Element Type

3.1.6. 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.

3.1.7. The NF shall support software upgrade.

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

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

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

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

3.1.12. The NF shall 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

4. General Requirements

4.1. Support of Multiple Equipment Vendors

The system shall support the possibility of using equipment and sub-systems of different vendors like AMF, SMF, UPF etc. as per defined industry standards, wherever relevant.

4.2. Software

4.2.1. The software shall be written in a High-Level Language. The software shall be modular and structured.

4.2.2. The software shall include the following characteristics:

4.2.2.1. The design of the software shall be such that the system is easy to handle both during installation and normal operations as well as during extensions.

4.2.2.2. The functional modularity of the software shall permit introduction of changes wherever necessary with least impact on other modules.

4.2.2.3. It shall be open-ended to allow addition of new features.

4.2.2.4. Adequate flexibility shall be available to easily adopt changes in service features & facilities and technological evolution in hardware.

4.2.2.5. The design shall be such that propagation of software faults is contained.

4.2.2.6. Test programs shall include fault tracing for detection and localization of system faults.

4.3. Software Maintenance

4.3.1. All software updates, for a period as specified, shall be supplied on continuing basis. These updates shall include new features and services and other maintenance updates.

4.3.2. Integration of software updates without posing any problem to the existing functionality shall be possible.

Chapter 8

5. Security Requirements

For all the NFs, the security requirements mentioned in the corresponding ITSAR (Indian Telecom Security Assurance requirements) of the NF shall be supported.

Chapter 9

6. ER of 5G Core

The clauses mentioned in the Essential Requirement (ER) of 5G Core, which are not covered in Chapter 1 to Chapter 8 in this document, shall also be supported by the corresponding NFs.

Chapter 10

7. Type Approval/ Technology Approval/ Certificate of Approval Requirements":

1. Field trial may be for a period of at least 3 weeks;
2. Demonstration/ submission of test reports (from TEC designated lab) for prescribed tests against all mandatory requirements;
3. Demonstration/ submission of test reports (from TEC designated lab) for prescribed tests against such optional requirements, if any, which are offered by the vendor voluntarily; and
4. Submission of required undertaking in respect of remaining prescribed tests, which are "optional and not offered voluntarily" or "Not Applicable".

Note: The equipment vendor shall specify the supported Networks Functions and indicate product specific configuration being offered for the type approval/technology approval.

Dimensioning

S. No.	Parameter	Option
1.	Number of gNodeB Supported	
2.	Number of UPF Supported	
3.	Number of slices Supported	
4.	Number of slices/UE Supported	
5.	Number of simultaneous registrations	
6.	Number of simultaneous PDU sessions	

Chapter 11

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.

Dimensioning

S. No.	Parameter	Option
7.	Number of gNodeB Supported	
8.	Number of UPF Supported	
9.	Number of slices Supported	
10.	Number of slices/UE Supported	
11.	Number of simultaneous registrations	
12.	Number of simultaneous PDU sessions	

Abbreviation

Abbreviation	Full Form
5G	Fifth Generation
5G-EIR	5G Equipment Identity Register
5GC	5G Core
AAA	Authentication, Authorization and Accounting
AAA-P	AAA Proxy
AAA-S	AAA Server
AANF	Access and Mobility Analytics Function
ADRF	Analytics Data Repository Function
AF	Application Function
AKA	Authentication and Key Agreement
AKMA	Authentication and Key Management for Applications
AMBR	Aggregate Maximum Bit Rate
AMF	Access and Mobility Management Function
API	Application Programming Interface
ASN.1	Abstract Syntax Notation One
AUSF	Authentication Server Function
BDT	Background Data Transfer
BSF	Binding Support Function
CBCF	Cell Broadcast Centre Function
CBS	Cell Broadcast Service
CDR	Charging Data Record
CH	Clearing House
CHF	Charging Function
CLI	Command Line Interface
CMIP	Common Management Information Protocol
CNC	Centralized Network Configuration
CNF	Cloud-native Network Function
CORBA	Common Object Request Broker Architecture
COTS	Commercial Off-The-Shelf
CPU	Central Processing Unit
CUPS	Control and User Plane Separation
DCCF	Data Collection Coordination Function

DCS	Data Clearing System
DDNMF	Direct Discovery Name Management Function
DL	Downlink
DN	Data Network
DNN	Data Network Name
DOT	Department of Telecommunications
DRA	Diameter Routing Agent
DSCP	Differentiated Services Code Point
EAP	Extensible Authentication Protocol
EASDF	Edge Application Server Discovery Function
EMC	Electromagnetic Compatibility
EMS	Element Management System
EPC	Evolved Packet Core
EPS	Evolved Packet System
ER	Essential Requirements
FBC	Flow Based Charging
FEC	Forward Error Correction
GBA	Generic Bootstrapping Architecture
GBFR	Guaranteed Flow Bit Rate
GBR	Guaranteed Bit Rate
GMLC	Gateway Mobile Location Centre
GNSS	Global Navigation Satellite System
GPSI	Generic Public Subscription Identifier
GR	Generic Requirements
GRE	Generic Routing Encapsulation
GSM	Global System for Mobile communications
GUI	Graphical User Interface
HGMLC	Home Gateway Mobile Location Centre
HLR	Home Location Register
HPLMN	Home Public Land Mobile Network
HSM	Hardware Security Module
HSS	Home Subscriber Server
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
I-SMF	Intermediate SMF
IE	Information Element

IEEE	Institute of Electrical and Electronics Engineers
IETF	Internet Engineering Task Force
IKE	Internet Key Exchange
IMEI	International Mobile Equipment Identity
IMS	IP Multimedia Subsystem
IMSI	International Mobile Subscriber Identity
IP	Internet Protocol
IPX	IP eXchange
IR	Interface Requirements
ISO	International Organization for Standardization
ITSAR	Indian Telecom Security Assurance Requirements
IWK	Interworking
KPI	Key Performance Indicator
K_TWIF	Key derived for TWIF (security key)
LAN	Local Area Network
LCS	Location Services
LDR	Location Deferred Request
LMF	Location Management Function
LTE	Long Term Evolution
MANO	Management and Orchestration
MB-SMF	Multicast Broadcast Session Management Function
MB-UPF	Multicast Broadcast User Plane Function
MBMS	Multimedia Broadcast Multicast Service
MBS	Multicast Broadcast Service
MBSF	Multicast Broadcast Service Function
MBSTF	MBS Traffic Handling Function
ME	Mobile Equipment
MFAF	Messaging Framework Adaptation Function
MFAP	Messaging Framework Adaptation Function (as written in document; elsewhere MFAF is used for the same function)
MFBR	Maximum Flow Bit Rate
MIB	Management Information Base
ML	Machine Learning
MME	Mobility Management Entity
MO-LR	Mobile Originated Location Request
MOBIKE	IKEv2 Mobility and Multihoming Protocol

MSISDN	Mobile Station International Subscriber Directory Number
MT-LR	Mobile Terminated Location Request
MT-SMS	Mobile Terminated Short Message Service
NAS	Non-Access Stratum
NE	Network Element
NEF	Network Exposure Function
NF	Network Function
NG-RAN	Next Generation Radio Access Network
NMS	Network Management System
NRF	Network Repository Function
NSAC	Network Slice Admission Control
NSACF	Network Slice Admission Control Function
NSSAAF	Network Slice-Specific Authentication and Authorization Function
NSSAI	Network Slice Selection Assistance Information
NSSF	Network Slice Selection Function
NSWOF	Non-Seamless WLAN Offload Function
NWDAF	Network Data Analytics Function
OAM	Operations, Administration and Maintenance
ODB	Operator Determined Barring
OMC	Operations and Maintenance Centre
P-CSCF	Proxy Call Session Control Function
PCC	Policy and Charging Control
PCF	Policy Control Function
PDN	Packet Data Network
PDU	Protocol Data Unit
PEI	Permanent Equipment Identifier
PFCP	Packet Forwarding Control Protocol
PLMN	Public Land Mobile Network
PM	Performance Management
PSA	PDU Session Anchor
QBC	QoS Flow Based Charging
QER	QoS Enforcement Rule
QFI	QoS Flow Identifier
QoS	Quality of Service
RAN	Radio Access Network
RAT	Radio Access Technology

RCS	Rich Communication Services
REST	Representational State Transfer
RFC	Request For Comments
RQI	Reflective QoS Indication
S-NSSAI	Single Network Slice Selection Assistance Information
SA	Standalone
SBA	Service-Based Architecture
SBI	Service-Based Interface
SCP	Service Communication Proxy
SDF	Service Data Flow
SEPP	Security Edge Protection Proxy
SFTP	Secure File Transfer Protocol
SGSN	Serving GPRS Support Node
SIM	Subscriber Identity Module
SMF	Session Management Function
SMS	Short Message Service
SMSF	Short Message Service Function
SNMP	Simple Network Management Protocol
SNPN	Standalone Non-Public Network
SPGW	Serving Gateway / PDN Gateway
SR	Service Requirements
SSH	Secure Shell
SUCI	Subscription Concealed Identifier
SUPI	Subscription Permanent Identifier
TA	Tracking Area
TAC	Type Allocation Code
TAI	Tracking Area Identity
TCP	Transmission Control Protocol
TEC	Telecommunication Engineering Centre
TMGI	Temporary Mobile Group Identity
TNAN	Trusted Non-3GPP Access Network
TNGF	Trusted Non-3GPP Gateway Function
TS	Technical Specification
TSC	Time Sensitive Communication
TSCTSF	Time Sensitive Communication Time Synchronization Function
TSN	Time Sensitive Networking

TTL	Time To Live
TWIF	Trusted WLAN Interworking Function
UCMF	UE Capability Management Function
UDM	Unified Data Management
UDR	Unified Data Repository
UDSF	Unstructured Data Storage Function
UE	User Equipment
UMTS	Universal Mobile Telecommunications System
UPF	User Plane Function
URI	Uniform Resource Identifier
URL	Uniform Resource Locator
URLLC	Ultra-Reliable Low-Latency Communication
URR	Usage Reporting Rule
V-NSSF	Visited NSSF
VGMLC	Visited GMLC
VNF	Virtual Network Function
VPLMN	Visited Public Land Mobile Network
WLAN	Wireless Local Area Network

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