सत्यमेव जयते

टेस्ट गाइड

टीईसी TEC २११२१:२०२५

TEST GUIDE

TEC 21121:2025

छोटेआकार का 5जी कोर

Small Size 5G Core

(**जीआर सं**: टी:सी २११२०.ई.२०२४**)**

(**GR No.:** TEC 21120:2024)

ISO 9001:2015

दूरसंचार अभियांत्रिकी केंद्र

दूरसंचार विभाग, संचार मंत्रालय, भारत सरकार

खुर्शीदलाल भवन, जनपथ, नई दिल्ली - ११०००१, भारत

TELECOMMUNICATION ENGINEERING CENTRE
DEPARTMENT OF TELECOMMUNICATIONS, MINISTRY OF COMMUNICATIONS GOVERNMENT OF INDIA, KHURSHIDLAL BHAWAN, JANPATH, NEW DELHI-110001, INDIA

www.tec.gov.in

Release1: XXXX, 2025

CONTENTS

A. INTRODUCTION

This document enumerates detailed test schedule and procedure for evaluating conformance / functionality / requirements / performance of Small Size 5G Core as per GR/IR/Applicant's spec. No GR No.: TEC 21120:2024

B. HISTORY SHEET

Sl. No.	TSTP No.	Equipment/Interface	Issue
1.	**TEST GUIDE No.: TEC: XXXXX:2025**	**Small Size 5G Core**	**Release No. 01**

C. General Information:

S. No.	General Information	Details	
1	Name, Address and Contact Details of the Applicant		
2	Date of Application		
3	Details of Equipment		
	Type of Equipment	Model No.	Serial No.
(i)			
(ii)			
4	Any other relevant Information: -		

D. Testing team:

S.No.	Name	Designation	Organization	Signature
1.				
2.				
3.				

E. List of the Test Instruments:

S.No.	Name of the test instrument	Make /Model	Validity of calibration
1			dd/mm/yyy
2			
3			

F. Equipment Configuration:

(i) *<Equipment/product name> Configuration:*

S.No.	Item	Details	Remarks

Relevant information like No. of cards, ports, slots, interfaces, size etc. may be filled as applicable for the product

G. Equipment/System Manuals:

Availability of Maintenance manuals, Installation manual, Repair manual & User Manual, any other technical manual etc. **(Y/N)**

H. Clause-wise Test Type and Test No.:

Clause No	Clause Description	Type of Test/ Test No. etc..
1.1	Overview This document contains standard for the Generic Requirements (GR) of "Small Size 5G Core" based mobile system which is a compact, cost effective, power efficient 5G SA (Stand-alone) Core targeted for Small size Networks, Temporary 5G Connectivity Requirements for Special Purposes, Disaster Management etc. for deployment in the Indian mobile communication network. The document covers the functional requirements, general requirements and features of the system. including OMC/EMC Requirements.	Informational
1.2	Objective The key objective of Small Size 5G Core is to have a compact, cost effective, power efficient which addresses the requirements in terms of coverage, capacity and quality with ease of deployment and ease of maintenance.	Informational
1.3	Applications As the system is small, compact 5G core, it may be suitable for providing the 5G mobile communication services, for the following applications as required: i. Small size Networks ii. Temporary 5G Connectivity Requirements for Special Purposes iii. Disaster Management	Informational
2	Small sized 5G Core The Small sized 5G Core Network utilizes service- based architecture (SBA) that spans across 5G functions and provides authentication, security, session management, mobility management connectivity and data access. The Network Functions (NFs) of the 5G Core Network are: 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) NOTE 1: In the case of Small Sized 5G Core, some of the NFs viz. BSF, CHF, NRF, NEF, NSSF etc. may or may not be required, depending on specific deployment. As such, all the above-mentioned NFs may not be required to be implemented. NOTE 2: The procurer is required to specify the NFs, which are needed based on their deployment scenario. NOTE 3: The manufacturer(s)/ vendor(s) are required to	Informational

	specify the NFs implemented in their system, while offering for testing/ certification for type approval/ technology approval/ certificate of approval.	
2.1	Interfaces for 5G Core network: This section describes an exhaustive list of 5G System service-based interfaces. The applicability of interfaces is enumerated in specific sections related to NFs.	Informational
3	Network Functions	Informational
3.1	AMF (Access and Mobility Management) AMF accesses the UE and the Radio Access Network in the signalling (control) plane	Informational
3.1.1	AMF functional requirements:	Informational
3.1.1.a	The AMF shall be capable of connecting to I) AUSF II) NG-RAN III) SMF IV) UDM	GR_TSTP_3.1.1_A
3.1.1.b	The AMF shall support:	
3.1.1.b.I	Primary authentication with AUSF using SUCI and SUPI for 5G AKA with SBI	GR_TSTP_3.1.1_B1
3.1.1.b.II	At least one 3GPP based option of Control Plane signalling confidentiality and integrity protection of NAS signalling.	GR_TSTP_3.1.1_B2
3.1.1.b.III	UE initiated PDU session release procedure in connected state	GR_TSTP_3.1.1_B3
3.1.1.b.IV	UE triggered service request procedure and respond with a service accept/reject message	GR_TSTP_3.1.1_B4
3.1.1.c	The AMF may support:	
3.1.1.c.I	Network initiated PDU session release procedure when the UE is in idle state.	GR_TSTP_3.1.1_C1
3.1.1.b.II	Rejecting PDU session establishment based on SUPI and DNN	GR_TSTP_3.1.1_C2
3.1.1.c.III	The AMF may provide the SMF with the PEI (Permanent Equipment Identifier) of the UE if the PEI is available with the AMF at the time of PDU session establishment	GR_TSTP_3.1.1_C3
3.1.1.c.IV	One CBCF or multiple CBCFs to provide PWS.	GR_TSTP_3.1.1_C4
3.1.1.c.V	Location services for transport for Location Services messages between UE and LMF as well as between RAN and LMF, in case of deployed disaster or temporary networks.	GR_TSTP_3.1.1_C5
3.1.1.c.VI	Roaming –Communication with the H-AUSF and H-UDM for authentication (N12 interface) and obtaining	GR_TSTP_3.1.1_C6

	subscription information (N8 interface).	
3.1.1.c.VII	The AMF may be capable of connecting to: I) PCF	GR_TSTP_3.1.1_C7
3.2.1.a	The SMF shall be capable of connecting to the I) AMF II) UPF UDM	GR_TSTP_3.2.1_A
3.2.1.b	The SMF may be capable of connecting to I) CHF II) PCF	GR_TSTP_3.2.1_B
3.2.1.c	The SMF shall support:	
3.2.1.c.I	Session establishment between UPF and NG-RAN node	GR_TSTP_3.2.1_C1
3.2.1.c.II	Selection and control of UPF function	GR_TSTP_3.2.1_C2
3.2.1.c.III	Deletion of the UE PDU session when it receives the request 1. The cause IE set to "REL_DUE_TO_DUPLICATE_SESSION_ID" from AMF; 2. The cause IE set to "REL_DUE_TO_SLICE_NOT_AVAILABLE" from AMF1 (Optional).	GR_TSTP_3.2.1_C3
3.2.1.c.IV	Allocation of IPv4 address and/or Ipv6 prefix based on subscription information received from UDM.	GR_TSTP_3.2.1_C4
3.2.1.d	The SMF may support:	
3.2.1.d.I	UE IP address allocation and management.	GR_TSTP_3.2.1_D1
3.2.1.d.II	Local UPF within a PDU session.	GR_TSTP_3.2.1_D2
3.2.1.d.III	Converged online and offline charging	GR_TSTP_3.2.1_D3
3.2.1.d.IV	Charging of PDU session using SBI interface	GR_TSTP_3.2.1_D4
3.2.1.d.V	CHF selection based on the Charging Characteristics or using NRF^2	GR_TSTP_3.2.1_D5
3.2.1.d.VI	Sending of Charging Data Request [Termination] when abort request is received from the CHF	GR_TSTP_3.2.1_D6
3.2.1.d.VII	Sending of Charging Data Request [update] and start new counts with time stamps at the start of new QoS flows which is not associated with default QoS rule.	GR_TSTP_3.2.1_D7
3.2.1.d.VIII	Sending of Charging Data Request [Update] and close the count with time stamp on expiry of time limit per PDU session.	GR_TSTP_3.2.1_D8
3.2.1.d.IX	Sending of Charging Data Request [Update] and close the count with time stamp on expiry of data volume	GR_TSTP_3.2.1_D9

	limit per PDU session.	
3.2.1.d.X	Not informing the AMF of DL Data notification if the SMF is aware that the UE is unreachable or if the UE is reachable only for prioritized services which does not include PDU session.	GR_TSTP_3.2.1_D10
3.2.1.d.XI	Roaming – Communication with H-SMF over N16 interface for PDU session establishment. [Note that the H-SMF interacts with the H-PCF for obtaining SM Policy and not the V-SMF]	GR_TSTP_3.2.1_D11
3.2.2	SMF QoS requirements:	Informational
3.2.2.a	The SMF shall support:	
3.2.2.a.I	QOS and Policy management support .~~Default QoS flows~~	GR_TSTP_3.2.2_A1_1
	Default QoS flows	GR_TSTP_3.2.2_A1_2
3.2.2.a.II	Dedicated QoS flows	GR_TSTP_3.2.2_A2
3.2.2.a.III	5QI values for eMBB	GR_TSTP_3.2.2_A3
3.2.2.a.IV	Minimum 1 QOS flow per UE. Upto 16 QoS flows per UE is optional	GR_TSTP_3.2.2_A4
3.2.2.a.V	Inclusion of GBFR and MFBR in QOS Profile for each GBR QoS Flow	GR_TSTP_3.2.2_A5
3.2.2.b	The SMF may support	
3.2.2.b.I	QoS handling on Flow level, Service level as well as Session level.	GR_TSTP_3.2.2_B1
3.2.2.b.II	Both pre-configured and/or dynamically assigned 5QI.	GR_TSTP_3.2.2_B2
3.2.2.b.III	Operator-specific 5QI in the range of 128-254.	GR_TSTP_3.2.2_B3
3.2.2.b.IV	QCI 65, 66, 69 and 70 - In case of support for MCX services	GR_TSTP_3.2.2_B4
3.2.2.b.V	Appropriate QCI values for URLLC use cases, depending on procurer requirement based on deployment scenario	GR_TSTP_3.2.2_B5
3.2.2.b.VI	Appropriate QCI values for mMTC use cases, depending on procurer requirement based on deployment scenario	GR_TSTP_3.2.2_B6
3.2.2.b.VII	Packet marking for HTTP/2 signaling over SBI.	GR_TSTP_3.2.2_B7
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)	Informational

3.3.1	UPF functional requirements:	Informational
3.3.1.a	The UPF shall be capable of connecting to the: I) SMF II) NG-RAN Data Network	GR_TSTP_3.3.1_A
3.3.1.b	The UPF shall support:	
3.3.1.b.I	Packet Detection based on predefined PDRs or PDRs received in the PFCP messages from the SMF over N4 interface	GR_TSTP_3.3.1_B1
3.3.1.b.II	A PDU session that carries IPv4 traffic	GR_TSTP_3.3.1_B2
3.3.1.b.III	QoS Flow ID (QFI) used to identify a QoS flow	GR_TSTP_3.3.1_B3
3.3.1.b.IV	User Plane Traffic to QoS flows based on the SDF templates	GR_TSTP_3.3.1_B4
3.3.1.c	The UPF may support:	
3.3.1.c.I	Buffering of packets instead of immediately forwarding them based on the instructions received from the control plane.	GR_TSTP_3.3.1_C1
3.3.1.c.II	Downlink Data Notification functionality.	GR_TSTP_3.3.1_C2
3.3.1.c.III	Monitoring the amount of downlink traffic that is dropped and report when a threshold is received as per the URR (Usage Reporting Rules) received from the SMF.	GR_TSTP_3.3.1_C3
3.3.1.c.IV	User Traffic Redirection based on Destination IP	GR_TSTP_3.3.1_C4
3.3.1.c.V	A PDU session that carries Ipv6 traffic.	GR_TSTP_3.3.1_C5
3.3.1.c.VI	Application detection.	GR_TSTP_3.3.1_C6
3.3.1.c.VII	Normalization of host server names in non-standard URLs in HTTP POST request messages so that HTTP post requests can be classified as standard requests.	GR_TSTP_3.3.1_C7
3.3.1.c.VIII	Tethering detection based on TTL values.	GR_TSTP_3.3.1_C8
3.3.1.c.IX	Multi-homed PDU session.	GR_TSTP_3.3.1_C9
3.3.1.c.X	HTTP Pipelining Request-Response matching enabling the user plane to match each HTTP response with the corresponding HTTP request.	GR_TSTP_3.3.1_C10
3.3.1.c.XI	Service chaining functionality allowing the user plane to steer subscriber traffic to third-party service functions in the N6 or Sgi-LAN.	GR_TSTP_3.3.1_C11
3.3.1.c.XII	Sending User Plane Inactivity Report to the SMF as a response when instructed.	GR_TSTP_3.3.1_C12

3.3.1.c.XIII	N4 session level report procedure based on Usage Report;	GR_TSTP_3.3.1_C13
3.3.1.c.XIV	N4 session level report procedure: I) Start of traffic detection; II) Stop of traffic detection; and III) Detection of PDU session inactivity for a specified period.	GR_TSTP_3.3.1_C14
3.3.1.c.XV	Roaming- Communication between visited UPF and Home UPF using the N9 interface.	GR_TSTP_3.3.1_C15
3.3.2	UPF QoS requirements:	Informational
3.3.2.a	The UPF shall support:	
3.3.2.a.I	Non-guaranteed flow bit rate QoS flows	GR_TSTP_3.3.2_A1
3.3.2.a.II	Enforcement of PDU session AMBR across all non-GBR QoS flows of a PDU session	GR_TSTP_3.3.2_A2
3.3.2.a.III	Dropping packets if any packet exceeds the limits of any of the associated QERs	GR_TSTP_3.3.2_A3
3.3.2.b	The UPF may support	
3.3.2.b.I	The QOS Flow for Guaranteed flow bit rate QoS flows;	GR_TSTP_3.3.2_B1
3.3.2.b.II	Transport level packet marking with a DSCP value.	GR_TSTP_3.3.2_B2
3.3.2.b.III	Inclusion of QFI and an indication for reflective QoS activation in the encapsulation header.	GR_TSTP_3.3.2_B3
3.3.2.b.IV	The Reflective QoS Indication (RQI) in the encapsulation header on N3 reference point together with the QFI.	GR_TSTP_3.3.2_B4
3.3.2.b.V	Marking of PDU session containers over the N3 interfaces with a QFI value that the control plane provides in a QER (QoS Enforcement Rule).	GR_TSTP_3.3.2_B5
3.4	UDM (Unified Data Management) Unified data management (UDM) is a centralized way to control network user data	Informational
3.4.1	UDM functional requirements:	Informational
3.4.1.a	UDM shall be connected with other 3GPP network elements using standard Interfaces I) SMF, N10 II) AMF, N8 AUSF, N13	GR_TSTP_3.4.1_A
3.4.1.b	UDM may be connected with other 3GPP network elements using standard Interfaces: I). SMSF, N21. II). UDR, N35;	GR_TSTP_3.4.1_B
3.4.1.c	The UDM shall support:	

3.4.1.c.I	Following high level features: 1. Identification and authentication;	GR_TSTP_3.4.1_C1
3.4.1.c.II	Maintenance of AMF/SMF registration session	GR_TSTP_3.4.1_C2
3.4.1.c.III	Sending of deregistration notification using Nudm_UECM_DeregistrationNotification to NF consumer	GR_TSTP_3.4.1_C3
3.4.1.c.IV	Data retrieval operation based on different query parameters (PLMN, NSSAI, DNN) and accordingly maintain session of subscriber	GR_TSTP_3.4.1_C4
3.4.1.c.V	UE Authentication to provide updated authentication related subscriber data to the subscribed NF consumer	GR_TSTP_3.4.1_C5
3.4.1.c.VI	Subscription of AMF and notify the AMF when subscription data is changed	GR_TSTP_3.4.1_C6
3.4.1.c.VII	Network-initiated deregistration requested by AMF using Nudm_UECM_DeregistrationNotification operation.	GR_TSTP_3.4.1_C7_1
3.4.1.c.VII	Following Authentication related features: 1. Generation of 3GPP AKA Authentication Credentials; 2. Selection of the 5G-AKA authentication method so that network Function Service Consumer (e.g. AMF) returns the result received from the UE to the AUSF; 3. Different protection scheme; Support of de-concealment of privacy-protected subscription identifier (SUCI);	GR_TSTP_3.4.1_C7_2
3.4.1.c.VIII	Following NRF services: 1. Nnrf_NFDiscovery service 2. NFRegister, NFUpdate, NFDeregister service 3. NF Heart-Beat service 4. Deletion of stale security context Use of NF discovery service on expiry of validity Period	GR_TSTP_3.4.1_C8
3.4.1.d	The UDM may support:	
3.4.1.d.I	Services (Get/Subscribe/ Unsubscribe/ Update) via the Nudm interface for subscriber data Management.	GR_TSTP_3.4.1_D1
3.4.1.d.II	The EAP-based authentication method;	GR_TSTP_3.4.1_D2
3.4.1.d.III	UDM data replication across multiple small size 5G Core network, which will enable UE to move from one small sized 5G Core network to another;	GR_TSTP_3.4.1_D3
3.4.1.d.IV	Following high level features: I) Network slice selection; II) Access control and barring; and III) Lawful Interception	GR_TSTP_3.4.1_D4
3.4.1.d.V	Generation and storage of keys using HSM to protect long-term keys from physical attacks and to keep them	GR_TSTP_3.4.1_D5

	in the secure environment.	
3.4.1.d.VI	Interworking with HSS: I) UDM shall provide support to Service based interfaces for direct UDM-HSS interworking; II) Terminating-Access Domain Selection for 5G access via UDM-HSS interworking; and III) P-CSCF restoration via UDM-HSS interworking.	GR_TSTP_3.4.1_D6
3.4.1.d.VII	Following Authentication related features: I) Support of MT-SMS delivery support services; and II) MT-SMS delivery support for short Message Roaming Routing, Set Message Waiting Data, Report SM-Delivery Status.	GR_TSTP_3.4.1_D7
3.4.1.d.VIII	NFStatusSubscribe, I)NFStatusNotify, NFStatusUnSubscribe service; II) NFListRetrieval service; III) NFProfileRetrieval service; IV) Nnrf_AccessToken service; and V) Validation of expire time present in token validation response from NRF.	GR_TSTP_3.4.1_D8
3.5	AuSF (Authentication Server Function) AuSF is responsible for the security procedure for SIM authentication using the 5G-AKA authentication method	Informational
3.5.1	AuSF functional requirements:	Informational
3.5.1.a	AuSF shall be connected with other 3GPP network elements using standard interfaces I) UDM, N13 AMF, N12	GR_TSTP_3.5.1_A
3.5.1.b	The AuSF shall support:	
3.5.1.b.I	At least one from Null, Profile-A or Profile-B.	GR_TSTP_3.5.1_B1
3.5.1.b.II	UE authentication service to the requester NF using Nausf_UEAuthentication	GR_TSTP_3.5.1_B2
3.5.1.b.III	Setting of the authResult to AUTHENTICATION FAILURE if the UE is not authenticated	GR_TSTP_3.5.1_B3
3.5.1.b.IV	5G-AKA procedures	GR_TSTP_3.5.1_B4
3.5.1.b.V	UE id (e.g. SUPI or SUCI), Serving Network Name in the “ authenticate” service request by NF	GR_TSTP_3.5.1_B5
3.5.1.b.VI	Provision of 4xx/5xx http status codes with message containing a Problem details structure with "cause" attribute set to one of the application error on failure in 5G –AKA and/or 5G-EAP-AKA’ procedure (5G-EAP-AKA’ procedure, if supported)	GR_TSTP_3.5.1_B6
3.5.1.b.VII	Following NRF services: 1. Nnrf_NFDiscovery service 2. NFRegister, NFUpdate and NFDeregister service	GR_TSTP_3.5.1_B7

	3. NF Heart-Beat service NFStatusSubscribe service and NFStatusNotify service	
3.5.1.c	The AuSF may support:	
3.5.1.c.I	5G-EAP-AKA procedures;	GR_TSTP_3.5.1_C1
3.5.1.c.II	Sending of NF access token request towards NRF after expiry of previous token: I) AUSF shall use NF discovery service on expiry of validity Period; and II) AUSF shall validate expire time present in token validation response from NRF.	GR_TSTP_3.5.1_C2
3.5.1.c.III	Both On-demand as well as Periodic/Scheduled backup procedures; (backup manual from the OMC/EMS)	GR_TSTP_3.5.1_C3
3.6	UDR (Unified Data Repository) UDR enables network functions to store and access subscription information. NOTE: In the case of Small Size 5G Core, UDR services may be applicable depending on procurer requirement based on deployment scenario.	Informational
3.6.1	UDR functional requirements :	
3.6.1.a	UDR shall be connected with other 3GPP network elements using standard service-based interface: I). UDM, N35; II). PCF, N25; and III).NEF, N37.	GR_TSTP_3.6.1_A
3.6.1.b	The UDR shall support:	
3.6.1.b.I	Authorization of user equipment.	GR_TSTP_3.6.1_B1
3.6.1.b.II	Storage of access and mobility data and session management data needed by NF consumers to implement application logic.	GR_TSTP_3.6.1_B2
3.6.1.b.III	Deletion of existing user data when a provisioning front end deletes a service profile for an existing user or profile for which consumer propose to remove an application data record.	GR_TSTP_3.6.1_B3
3.6.1.b.IV	Storage of new user data from NF service consumer, e.g., when a provisioning Front end consumer creates a profile for a new user or creates a new service profile for an existing user, or NF service consumer intends to insert a new application data record into the UDR.	GR_TSTP_3.6.1_B4
3.6.1.b.V	Authorization management mechanism to guarantee the safety of data access also access control in terms of read/write and level of service data to be accessed.	GR_TSTP_3.6.1_B5
3.6.1.b.VI	User confidentiality protection functionalities: (I) Providing globally unique 5G Subscription	GR_TSTP_3.6.1_B6_1 GR_TSTP_3.6.1_B6_2

	Permanent Identifier (SUPI) to each subscriber in the 5G System and provisioned in the UDM/UDR; (II) Supporting Permanent Equipment Identifier (PEI) to assume different formats for different UE types and use cases; (III) And HTTP GET and HTTP POST method for Query and subscribe operation; and (IV) Ability to identify and remove inconsistent data.	
3.6.1.c	The UDR may support:	
3.6.1.c.I	Nudr_DataRepository services - Service operations like Create, Delete, Update, Notify, Subscribe, unsubscribe;	GR_TSTP_3.6.1_C1
3.6.1.c.II	User confidentiality protection functionalities: I) Monitoring of various events configured via UDM	GR_TSTP_3.6.1_C2
3.6.1.c.III	Load Balancing Functionalities: (I) Supporting overload protections within UDR architecture and implementation to prevent processing overload of the UDR from application layer; (II) Providing redundancy models for each load balancing; and (III) An overload threshold value shall be set. Once the UDR loading reaches the threshold value, the system shall generate alarms before service impact.	GR_TSTP_3.6.1_C3
3.6.1.c.IV	Different Redundancy mechanism procedures: (I) The UDR system redundancy shall support several levels of redundancy like data redundancy, site level redundancy, Network redundancy; (II) UDR shall support High-Availability to guarantee carrier-grade 99.999% system availability and avoid any Single Point of Failure; and (III) 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.	GR_TSTP_3.6.1_C4
3.6.1.c.V	1+1 or 1+1+1 redundancy at data service level.	GR_TSTP_3.6.1_C5
3.6.1.c.VI	Following NRF services:5 (Optional) (I) NFStatusSubscribe, NFStatusUnsubscribe, NFRegister; (II) NFUpdate, NFDeregister, NFListRetrieval, NFProfileRetrieval; (III) Nnrf_AccessToken service, Heat Beat Service	GR_TSTP_3.6.1_C6

	mechanism; (IV) Nnrf_NFManagement service; and (V) Nnrf_NFDiscovery service.	
3.7	NRF (Network Repository Function) NRF controls, the other Network Functions (NFs) by providing support for NF register, deregister and update service to NF and their services. NOTE: In the case of Small Size 5G Core, NRF services may be applicable depending on procurer requirement based on deployment scenario.	Information
3.7.1	NRF functional requirements:	
3.7.1.a	a. NRF shall be connected with other 3GPP network elements using standard Service Based Interface (SBI) (I) AMF; (II) SMF (III) UDM; (IV) AUSF; (V) NEF; (VI) PCF; and (VII) NSSF.	GR_TSTP_3.7.1_A
3.7.1.b	NRF may be connected with other 3GPP network elements using standard Service Based Interface (SBI) (I) SMSF; (II) UPF.	GR_TSTP_3.7.1_B
3.7.1.c	The NRF shall support:	
3.7.1.c.I	Following services: (I) Nnrf_NFManagement service; (II) Nnrf_NFDiscovery service; (III) NFRegister service; (IV) NFUpdate service; (V) NF Heart-Beat service; (VI) NFDeregister service; (VII) NFStatusSubscribe service; (VIII) NFStatusNotify service; (IX) NFStatusUnSubscribe service;	GR_TSTP_3.7.1_C1
3.7.1.c.II	Subscription and notification to other NFs regarding the registration in NRF of new NF instances of a given type.	GR_TSTP_3.7.1_C2
3.7.1.c.III	Subscription of NF to be notified of registration, deregistration and profile changes of NF Instances, along with their potential NF services	GR_TSTP_3.7.1_C3
3.7.1.c.IV	Nnrf_NFManagement service to allow NF to retrieve a list of NF and SCP Instances currently registered in the NRF or the NF Profile of a given NF Instance.	GR_TSTP_3.7.1_C4
3.7.1.c.V	NF Register Service. It allows an NF or SCP Instance to register its profile in the NRF; it includes the registration of the general parameters of the NF Instance, together with the list of potential services	GR_TSTP_3.7.1_C5

	exposed by the NF Instance.	
3.7.1.c.VI	Support for NFDeregister Service request.	GR_TSTP_3.7.1_C6
3.7.1.d	NRF may support:	
3.7.1.d.I	Following services: (I) Nnrf_AccessToken service; (II) Nnrf_Bootstrapping service (III) NFListRetrieval service; and (IV) NFProfileRetrieval service	GR_TSTP_3.7.1_D1
3.7.1.d.II	Deployment on shared-slice level (the NRF is configured with information belonging to a set of Network Slices).	GR_TSTP_3.7.1_D2
3.7.1.d.III	Data structures and URI query parameters as defined in 3GPP TS 29.510 Clause 6.1.3.2.3.1.	GR_TSTP_3.7.1_D3
3.7.1.d.IV	Ability to send requests to SEPP in weighted or priority mode or combination of these.	GR_TSTP_3.7.1_D4
3.7.1.d.V	Blocking of Register operation to be invoked from an NRF in a different PLMN.	GR_TSTP_3.7.1_D5
3.7.1.d.VI	Configuration with multiple PLMN IDs and registering, updating and deregistering the profile of Network Function Instances from any of these PLMN IDs.	GR_TSTP_3.7.1_D6
3.7.1.d.VII	Changing the NFStatus of a NF to SUSPENDED if the NRF detects that the NF is no longer operative using the NF Heart-Beat procedure or by update procedure if the NF is still operative as per 3GPP TS 29.510 Section 5.2.2.3.2	GR_TSTP_3.7.1_D7
3.7.1.d.VIII	Forwarding subscription request on basis of (target) PLMN-ID & NF-type if pre-configured routing policy is present. Precedence shall be given to routing Policy.	GR_TSTP_3.7.1_D8
3.7.1.d.IX	Sending of POST request directly from NRF-2 to the NF Service Consumer without involvement of NRF-1 for Notification for subscription via Intermediate NRF.	GR_TSTP_3.7.1_D9
3.7.1.d.X	Forwarding request to locally configured/registered forwarding NRF of same PLMN, in case of multiple NRF scenario. NRF2 shall send “307 temporary redirect” response to NRF1 containing location header of service producer NRF (If available locally otherwise 404). NRF1 shall re-initiate request to NRF3 and shall forward response towards requester NF as per 3GPP TS 29.510 Section 5.4.2.2.3.	GR_TSTP_3.7.1_D10
3.7.1.d.XI	Generic data of each NF Instance, applicable to any NF type, and it may also contain NF-specific data, for those NF Instances belonging to a specific type (e.g., the attribute “udrInfo” is typically present in the NF Profile when the type of the NF Instance takes the value “UDR”) in NF Profile object returned in	GR_TSTP_3.7.1_D11

	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.	
3.7.1.d.XII	Multiple level of recovery from software and hardware faults such that the impact on system operation shall be in accordance to the severity of the faults. In other words, not all software or hardware faults shall cause system or application recovery that has system wide impact.	GR_TSTP_3.7.1_D12
3.7.1.d.XIII	Establishment of connection with Secondary SEPP IP for forwarding the same request, in case when request timeout is received from Primary SEPP IP.	GR_TSTP_3.7.1_D13
3.7.1.d.XIV	Geo-redundancy and disaster recovery architecture without any data loss or service outage.	GR_TSTP_3.7.1_D14
3.7.1.d.XV	Roaming - Communication with H-NRF to resolve the home PLMN network functions over N27 interface via SEPP.	GR_TSTP_3.7.1_D15
3.8	PCF (Policy Control Function) PCF controls that the user data traffic does not exceed the negotiated bearer(s) capacities. NOTE: In the case of Small Size 5G Core, PCF services may be applicable depending on procurer requirement based on deployment scenario.	Informational
3.8.1	PCF functional requirements:	
3.8.1.a	The PCF shall support:	
3.8.1.a.I	Interactions with the access and mobility policy enforcement in the AMF, through service-based interfaces.	GR_TSTP_3.8.1_A1
3.8.1.a.II	Decision taking based upon subscription information, Access Type and the RAT Type.	GR_TSTP_3.8.1_A2
3.8.1.a.III	Handling of UE Context Establishment request as a part of UE Registration.	GR_TSTP_3.8.1_A3
3.8.1.a.IV	The capability to take a PCC rule into service, and out of service, at a specific time of day	GR_TSTP_3.8.1_A4
3.8.1.a.V	Session management related functionality of PDU Session related policy control.	GR_TSTP_3.8.1_A5
3.8.1.a.VI	The capability to indicate to the SMF that a PCC rule shall be bound to the specified QoS flow (including default QoS flow).	GR_TSTP_3.8.1_A6
3.8.1.a.VII	Control of QoS for the packet traffic of the PDU Session.	GR_TSTP_3.8.1_A7
3.8.1.a.VII	Mechanism to initiate QoS Flow establishment and modification as part of the QoS control.	GR_TSTP_3.8.1_A8
3.8.1.b	Handling QoS Flows that require a guaranteed bitrate (GBR bearers) and QoS Flows for which there is no guaranteed bitrate (non-GBR bearers).	GR_TSTP_3.8.1_B

3.8.1.c	The PCF may support:	
3.8.1.c.I	Utilization of the locally configured operator policies to make authorization and policy decisions, if the UE IP address belongs to an emergency DNN. The PCF shall not perform subscription check in this case.	GR_TSTP_3.8.1_C1
3.8.1.c.II	Charging control, policy control or both for a DNN access.	GR_TSTP_3.8.1_C2
3.8.1.c.III	Session management related functionality of Policy and charging control for a service data flow.	GR_TSTP_3.8.1_C3
3.8.1.c.IV	Selective Blocking of RCS Services based on PLMN, TAI and Postpaid/Prepaid Subscription.	GR_TSTP_3.8.1_C4
3.8.1.c.V	SmPolicyDecision data structure to provide the revalidation time within the "revalidationTime" attribute and the RE_TIMEOUT policy control request trigger within the "policyCtrlReqTriggers" attribute to instruct the SMF to trigger a PCF interaction to request PCC rule from the PCF as per 3GPP TS 23.503.	GR_TSTP_3.8.1_C5
3.8.1.c.VI	During the lifetime of the PDU session, within the SmPolicyDecision data structure, the PCF may provide the revalidation time within the "revalidationTime" attribute and the RE_TIMEOUT policy control request trigger within the "policyCtrlReqTriggers" attribute to instruct the SMF to trigger a PCF interaction to request PCC rule from the PCF, if not provided yet.	GR_TSTP_3.8.1_C6
3.8.1.c.VII	Session binding, which shall take the following IP CAN parameters into account: (I) The UE IPv4 address and/or IPv6 network prefix; (II) The UE identity, if present; and (III) The information about the packet data network (PDF) the user is	GR_TSTP_3.8.1_C7
3.8.1.c.VIII	Data barring based on PLMN and TAC (Type allocation code in IMEI);	GR_TSTP_3.8.1_C8
3.8.1.c.IX	Modification of the authorized Session AMBR at any time during the lifetime of the PDU session and provision it to the SMF; and	GR_TSTP_3.8.1_C9
3.8.1.c.X	Modification of the authorized Default QoS during the lifetime of the PDU session and provision it to the SMF.	GR_TSTP_3.8.1_C10
3.8.1.c.XI	Roaming - Communication with H-PCF over N24 interface for obtaining relevant UE Policy via SEPP.	GR_TSTP_3.8.1_C11
3.9	NEF (Network Exposure Function) NEF provides a means to securely expose the services and capabilities provided by 3GPP Network Functions. NOTE: In the case of Small Size 5G Core, NEF services may be applicable depending on procurer requirement based on deployment scenario.	Informational

3.9.1	NEF functional requirements:	
3.9.1.a	The NEF shall be connected with other 3GPP network elements using standard Service based interface (I) NRF; (II) BSF; (III) PCF, N30; and (IV) AF, N33.	GR_TSTP_3.9.1_A
3.9.1.b	The NEF shall support: (I) Service-based interface Nnef	GR_TSTP_3.9.1_B
3.9.1.c	The NEF may support:	
3.9.1.c.I	Masking of network and user sensitive information to external AF's according to the network policy.	GR_TSTP_3.9.1_C1
3.9.1.c.II	Procedure for resource management of Background Data Transfer (BDT).	GR_TSTP_3.9.1_C2
3.9.1.c.III	Resource Management of BDT API for background data transfer.	GR_TSTP_3.9.1_C3
3.9.1.c.IV	Nnef_TrafficInfluence service, Nnef_AFsessionWithQoS service	GR_TSTP_3.9.1_C4
3.9.1.c.V	Authentication of the Application Functions, authorization of Application Functions, throttling of the Application Functions, exposure of monitoring capabilities, exposure of provisioning capabilities, policy/charging capabilities.	GR_TSTP_3.9.1_C5
3.9.1.c.VI	Sending a GET request to the UDM to receive the SUPI that corresponds to the provided GPSI. The request contains the UE's identity (GPSI) and the type of the requested information.	GR_TSTP_3.9.1_C6
3.9.1.c.VII	Nnef_BDTPNegotiation service, Nnef_ChargeableParty service, NF_management operations with NRF, exposure of bulk subscription.	GR_TSTP_3.9.1_C7
3.9.1.c.VIII	Translation of information exchanged with the AF and information exchanged with the internal network function.	GR_TSTP_3.9.1_C8
3.9.1.d	NEF may be connected to UDR, using standard Service based interface N37.	GR_TSTP_3.9.1_D
3.10	NSSF (Network Slicing Selection Function) NSSF provides a solution to select the optimal network slice available for the service requested by the user in the 5G environment, where various services are provided. NOTE: In the case of Small Size 5G Core, NSSF services may be applicable depending on procurer requirement based on deployment scenario.	Informational
3.10.1	NSSF functional requirements:	Informational
3.10.1.a	NSSF shall be connected with other 3GPP network elements, viz. NRF and AMF, using Standard Service-	GR_TSTP_3.10.1_A

	based Interface.	
3.10.1.b	NSSF may be connected with other 3GPP network elements, viz. EMS using Standard Service-based Interface	GR_TSTP_3.10.1_B
3.10.1.c	The NSSF shall support:	
3.10.1.c.I	Determination of the Allowed NSSAI.	GR_TSTP_3.10.1_C1
3.10.1.c.II	Single UE access to one or more Network Slice Instance	GR_TSTP_3.10.1_C2
3.10.1.c.III	Selection of same AMF for different set of slices.	GR_TSTP_3.10.1_C3
3.10.1.c.IV	Nnssf_NSSelection for slice-info-request-for-registration to provide the Allowed NSSAI, configured NSSAI and may provide AMF set or the list of candidate AMF information to the Requester in Roaming scenarios and, if needed, mapping to the Subscribed S-NSSAIs.	GR_TSTP_3.10.1_C4
3.10.1.c.V	Provision of configured slice information for the PLMN when requested with “default configured S-NSSAI “indication.	GR_TSTP_3.10.1_C5
3.10.1.c.VI	Availability Service to provide AuthorizedNssaiAvailabilityInfo slice that is available per TAI for the S-NSSAIs the NF service consumer supports.	GR_TSTP_3.10.1_C6
3.10.1.c.VII	Following services: (I) NFRegister service; (II) NFDeregister service; and (III) NFStatusNotify service.	GR_TSTP_3.10.1_C7
3.10.1.d	The NSSF may support following services: (I) NFStatusSubscribe service; and (II) NFProfileRetrieval service.	GR_TSTP_3.10.1_D
3.10.1.e	NSSF may support	
3.10.1.e.I	Nnssf_NSSAIAvailability delete service operation for deletion of availability of S-NSSAIs per TA.	GR_TSTP_3.10.1_E1
3.10.1.e.II	The capability to provide bulk provisioning over all exposed interfaces. It shall provide Real time subscriber data synchronization.	GR_TSTP_3.10.1_E2
3.10.1.e.III	Roaming - Communication with the H-NSSF for selection of the S-NSSAI applicable in the case of roaming.	GR_TSTP_3.10.1_E3
3.11	BSF (Binding Support Function) BSF is used for binding an application-function request to a specific PCF instance. NOTE: In the case of Small Size 5G Core, BSF services may be applicable depending on procurer requirement based on deployment scenario.	Informational

3.11.1	BSF functional requirements:	
3.11.1.a	The BSF shall be compliant with 3GPP TS 29.521 "Binding Support Management service".	GR_TSTP_3.11.1_A
3.11.1.b	The BSF shall support:	
3.11.1.b.I	Registration of BSF profile with NRF, if NRF is available/part of the 5G compact mobile system.	GR_TSTP_3.11.1_B1
3.11.1.b.II	Heartbeat procedure periodically with NRF to update NF status. This heartbeat message shall also include BSF load information, if NRF is available/part of the 5G compact mobile system.	GR_TSTP_3.11.1_B2
3.11.1.b.III	Discovery of BSF via Nnrf_Discovery API by the NF Consumers (NEF or AF), if NRF is available/part of the 5G compact mobile system.	GR_TSTP_3.11.1_B3
3.11.1.b.IV	Creation, storage, updation and deletion of session binding information with various parameters such as UE address, PCF ID, DNN, SUPI or SNSSAI.	GR_TSTP_3.11.1_B4
3.11.1.b.V	Binding between PCF and NEF or AF.	GR_TSTP_3.11.1_B5
3.11.2	BSF QoS requirements	
3.11.2.a	The BSF shall support:	
3.11.2.a.I	Use of Nbsf_Management_Register, Nbsf_Management_Deregister and Nbsf_Management_Update service operations by PCF; and	GR_TSTP_3.11.2_A1
3.11.2.a.II	Nbsf_Management_Register, Nbsf_Management_Deregister and, Nbsf_Management_Update to register, deregister and update binding information into the BSF	GR_TSTP_3.11.2_A2
3.11.2.a.III	Use of Nbsf_Management_Deregister service operation to delete binding information when Policy Association Termination is initiated by the SMF and PCF.	GR_TSTP_3.11.2_A3
3.11.2.a.IV	Use of Nbsf_Management_Deregister service operation to delete binding information when Policy Association Termination is initiated by the PCF.	GR_TSTP_3.11.2_A4
3.11.2.b	The BSF may support:	
3.11.2.b.I	Use of Nbsf_Management_Discovery service operation to obtain the selected PCF id for a PDU session by a client NEF, NWDAF, AF, IMS, DRA). BSF responds with the PCF id and others related binding information.	GR_TSTP_3.11.2_B1
3.12	CHF (Charging Function) CHF allows charging services to be offered to authorized network functions.	Informational

	NOTE:In the case of Small Size 5G Core, CHF services may be applicable depending on procurer requirement based on deployment scenario.	
3.12.1	CHF functional requirements:	
3.12.1.a	The CHF shall support:	
3.12.1.a.I	Following charging features: (I) Usage based charging; (II) Speed based charging/ Quality of service charging; (III) Application ID charging; (IV) Network slice-based charging on 5G; (V) URL based charging.	GR_TSTP_3.12.1_A1
3.12.1.a.II	converged online charging and offline charging functionalities. The CHF provides the following: (I) Quota; (II) Re-authorization triggers; (III) Receiving service usage reports from NF Service Consumer; and (IV) CDRs generation.	GR_TSTP_3.12.1_A2
3.12.1.a.III	N40 interface with the SMF for Data Connectivity Charging, which includes: (I) Flow based charging (FBC); and (II) QoS Flow based Charging (QBC).	GR_TSTP_3.12.1_A3
3.12.1.a.IV	Time-based, volume-based and event-based charging and any such combination.	GR_TSTP_3.12.1_A4
3.12.1.a.V	3GPP specified services;	GR_TSTP_3.12.1_A5
3.12.1.a.VI	Consumption of services exposed by the NRF;	GR_TSTP_3.12.1_A6
3.12.1.a.VII	5G defined new identities: GPSI (MSISDN) and SUPI (IMSI);	GR_TSTP_3.12.1_A7
3.12.1.a.VIII	Charging based on supported 5G network architectures such as Multiple IP Address, Multiple Slices, Multiple Identifiers across Networks, No phone number, on-net vs roaming, etc;	GR_TSTP_3.12.1_A8
3.12.1.a.IX	Charging Data Record (CDR) file format and transfer and Charging Data Record (CDR) parameter description as per 3GPP specifications. The output CDR format may be compliant to ASN.1 structure as per 3GPP specification; and	GR_TSTP_3.12.1_A9
3.12.1.a.X	Upgradeability to 3GPP Rel-16 functionality and also backward compatibility;	GR_TSTP_3.12.1_A10
3.12.1.a.XI	All mandatory fields for CDR in 3GPP TS32.255;	GR_TSTP_3.12.1_A11
3.12.1.a.XII	Nchf_ConvergedCharging request message containing different multipleUnitUsage information and reply with multipleUnitInformation, associated to several	GR_TSTP_3.12.1_A12

	Rating Groups being accessed during the PDU session and which may be managed with different charging methods (online or offline).	
3.12.1.a.XIII	Charging of roaming traffic.	GR_TSTP_3.12.1_A13
3.12.1.a.XIV	Following interface functions from CHF perspective:	GR_TSTP_3.12.1_A14
3.12.1.a.XV	Support Interface with AMF/SGSN/MME/SMF/UPF/SPGW; and	GR_TSTP_3.12.1_A15
3.12.1.a.XVI	CHF to Register/update/deregister towards NRF.	GR_TSTP_3.12.1_A16
3.12.1.a.XVII	Converged online and offline charging triggered from Session Management Function (SMF).	GR_TSTP_3.12.1_A17
3.12.1.a.XVIII	Following notification requirements –	GR_TSTP_3.12.1_A18
3.12.1.a.XIX	Nchf_ConvergedCharging_Create/Delete /Notify; and	GR_TSTP_3.12.1_A19
3.12.1.a.XX	Nchf_SpendingLimitControl_Subscribe/Unsubscribe/Notify.	GR_TSTP_3.12.1_A20
3.12.1.a.XXI	Different charging between 4G and 5G.	GR_TSTP_3.12.1_A21
3.12.1.b	The CHF may support:	
3.12.1.b.I	Charging of 5G sessions in case of session and service continuity mode, as defined in TS 32.255.	GR_TSTP_3.12.1_B1
3.12.1.b.II	Spending Limit Control Service of the Nchf Service according to TS 32.290 and TS 29.504	GR_TSTP_3.12.1_B2
3.12.2	CHF QoS requirements:	Informational
3.12.2.a.I	QoS flow-based Charging (QBC), where data volumes are collected per user and per PDU session and categorized per QoS Flow identified by its QoS Flow Identifier (QFI).	GR_TSTP_3.12.2_A1
3.12.2.a.II	Flow-based charging (FBC) where data volumes are collected per user and per PDU session and categorized per rating group or per combination of rating group/service identifier related to one or more individual service data flows.	GR_TSTP_3.12.2_A2
3.12.2.a.III	Integration of 4G Charging and 5G charging.	GR_TSTP_3.12.2_A3
3.12.2.a.IV	Charging of services based on network slice, as well as charging as per network slice management.	GR_TSTP_3.12.2_A4
3.12.2.a.V	PDU session charging (data volumes are collected per user and per PDU session).	GR_TSTP_3.12.2_A5
3.13	SMSF (Short Message Service Function) SMSF is required for the provision of SMS over NAS through AMF. Optionally, SMS service may be offered through use of IMS. NOTE: In the case of Small Size 5G Core, SMSF	Informational

	services may be applicable depending on procurer requirement based on deployment scenario.	
3.13.a	The SMSF may support convergent charging towards CHF.	GR_TSTP_3.13_A
3.14	NWDAF (Network Data Analytics Function) NWDAF is a NF used to collect data from user equipment, network functions, and operations, administration, and maintenance (OAM) systems, etc. NOTE: In the case of Small Size 5G Core, NWDAF services may be applicable depending on procurer requirement based on deployment scenario.	Informational
3.14.a	The NWDAF shall support one or more of the following functionalities:	
3.14.a.I	Identifier of network slice instance.	GR_TSTP_3.14_A1
3.14.a.II	Load level information for that network slice instance.	GR_TSTP_3.14_A2
3.14.a.III	Support data collection from NFs and AFs.	GR_TSTP_3.14_A3
3.14.a.IV	Support data collection from OAM.	GR_TSTP_3.14_A4
3.14.a.V	NWDAF service registration and metadata exposure to NFs and Afs	GR_TSTP_3.14_A5
3.14.a.VI	Support analytics information provisioning to NFs and AFs.	GR_TSTP_3.14_A6
3.14.a.VII	Support Machine Learning (ML) model training and provisioning to NWDAFs (containing Analytics logical function).	GR_TSTP_3.14_A7
3.14.b	The NWDAF may allow NF consumers to subscribe to and unsubscribe from periodic notification and/or notification when a threshold is exceeded.	GR_TSTP_3.14_B
3.15	SEPP (Security Edge Protection Proxy) SEPP is required to manage the connectivity in trusted mode and to ensure that the exchange of information (signalling) among Operators may take place in a confidential, secure and robust way, aiming to protect against malicious attempts or attacks on data confidentiality, identity spoofing or information tampering. NOTE: In the case of Small Size 5G Core, SEPP services may be applicable depending on procurer requirement based on deployment scenario.	Informational
3.15.a	The SEPP is a non-transparent proxy and shall support:	
3.15.a.I	Message filtering and policing on inter-PLMN control plane interfaces. NOTE: The SEPP protects the connection between Service Consumers and Service Producers from a security perspective, i.e., the SEPP does not duplicate	GR_TSTP_3.15_A1

	the Service Authorization applied by the Service Producers.	
3.15.a.II	Topology hiding. The SEPP applies the functionality to every Control Plane message in inter-PLMN signalling, acting as a service relay between the actual Service Producer and the actual Service Consumer. For both Service Producer and Consumer, the result of the service relaying is equivalent to a direct service interaction. Every Control Plane message in inter-PLMN signalling between the SEPPs may pass via IPX entities.	GR_TSTP_3.15_A2
3.15.a.III	N32 interface	GR_TSTP_3.15_A3
3.16	SCP (Service Communication Proxy) SCP is the routing control point that mediates all Signalling and Control Plane messages in the network core. NOTE: In the case of Small Size 5G Core, SCP services may be applicable depending on procurer requirement based on deployment scenario.	Informational
3.16.a	The SCP shall support load balancing, monitoring, overload control etc.	GR_TSTP_3.16_A
3.16.b	The SCP includes one or more of the following functionalities: (I) Indirect Communication; (II) Delegated Discovery; (III) Message forwarding and routing to destination NF/NF service; and (IV) Message forwarding and routing to a next hop SCP NOTE: Some or all of the SCP functionalities may be supported in a single instance of an SCP:	GR_TSTP_3.16_B
3.16.c	The SCP may support communication security (e.g. authorization of the NF Service Consumer to access the NF Service Producer API).	GR_TSTP_3.16_C
3.17	N3IWF (Non-3GPP Interworking Function) N3IWF acts as a gateway for the 5GC with support for N2 and N3 interface towards the 5GC. NOTE: In the case of Small Size 5G Core, N3IWF services may be applicable depending on procurer requirement based on deployment scenario.	Informational
3.17.a	The N3IWF shall support:	
3.17.a.I	Support of IPsec tunnel establishment with the UE: The N3IWF terminates the IKEv2/IPsec protocols with the UE over NWu and relays over N2 the information needed to authenticate the UE and authorize its access to the 5G Core Network.	GR_TSTP_3.17_A1
3.17.a.II	Termination of N2 and N3 interfaces to 5G Core Network for control - plane and user-plane	GR_TSTP_3.17_A2

	respectively.	
3.17.a.III	Relaying uplink and downlink control-plane NAS (N1) signalling between the UE and AMF.	GR_TSTP_3.17_A3
3.17.a.IV	Handling of N2 signalling from SMF (relayed by AMF) related to PDU Sessions and QoS.	GR_TSTP_3.17_A4
3.17.a.V	Establishment of IPsec Security Association (IPsec SA) to support PDU Session traffic.	GR_TSTP_3.17_A5
3.17.a.VI	Relaying uplink and downlink user-plane packets between the UE and UPF. This involves: (I) De-capsulation/ encapsulation of packets for IPSec and N3 tunnelling; (II) 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; (III) Local mobility anchor within untrusted non-3GPP access networks using MOBIKE per IETF RFC 4555;	GR_TSTP_3.17_A6
3.18	LMF The LMF manages the overall co-ordination and scheduling of resources required for the location of a UE that is registered with or accessing 5GCN. It also calculates or verifies a final location and any velocity estimate and may estimate the achieved accuracy. NOTE: In the case of Small Size 5G Core, Location services may be applicable depending on procurer requirement based on deployment scenario.	Informational
3.18.a	The LMF shall:	
3.18.a.I	Determine the result of the positioning in geographical co-ordinates as defined in TS 23.032. If requested and if available, the positioning result may also include the velocity of the UE.	GR_TSTP_3.18_A1
3.18.b	The LMF may support:	
3.18.b.I	Request for a single location received from a serving AMF for a target UE.	GR_TSTP_3.18_B1
3.18.b.II	Request for periodic or triggered location received from a serving AMF for a target UE.	GR_TSTP_3.18_B2
3.18.b.III	Determination of position methods based on UE and PLMN capabilities, QoS, UE connectivity state per access type and LCS Client type.	GR_TSTP_3.18_B3
3.18.b.IV	Report of UE location estimates directly to a GMLC for periodic or triggered location of a target UE.	GR_TSTP_3.18_B4
3.18.b.V	Cancelation of periodic or triggered location for a target UE.	GR_TSTP_3.18_B5
3.18.b.VI	Provision of broadcast assistance data to UEs via NG-RAN in ciphered or unciphered form and forward any	GR_TSTP_3.18_B6

	ciphering keys to subscribed UEs via the AMF.	
3.18.b.VII	Change of a serving LMF for periodic or triggered location reporting for a target UE.	GR_TSTP_3.18_B7
3.19	CBCF CBCF is used in Public Warning System (PWS) for cell broadcast of CBS messages and acts as manager between the Cell broadcast Entity that generates the message and the AMF that further transmits it to the UE through the NG-RAN. NOTE: In the case of Small Size 5G Core, PWS services may be applicable depending on procurer requirement based on deployment scenario.	Informational
3.19.a	The CBCF shall support:	
3.19.a.I	The CBCF shall be responsible for the management of CBS messages	GR_TSTP_3.19_A1
3.19.a.II	Allocation of serial numbers;	GR_TSTP_3.19_A2
3.19.a.III	Modifying or deleting CBS messages held by the NG-RAN node;	GR_TSTP_3.19_A3
3.19.a.IV	Initiating broadcast by sending fixed length CBS messages to a NG-RAN node for each language provided by the cell, and where necessary padding the pages to a length of 82 octets (see 3GPP TS 23.038 [3]);	GR_TSTP_3.19_A4
3.19.a.V	Determining the set of cells to which a CBS message should be broadcast, and indicating within the Serial Number the geographical scope of each CBS message;	GR_TSTP_3.19_A5
3.19.a.VI	Determining the time at which a CBS message should commence being broadcast;	GR_TSTP_3.19_A6
3.19.a.VII	Determining the time at which a CBS message should cease being broadcast and subsequently instructing each NG-RAN node to cease broadcast of the CBS message;	GR_TSTP_3.19_A7
3.19.a.VIII	Determining the period at which broadcast of the CBS message should be repeated;	GR_TSTP_3.19_A8
3.19.a.IX	When CBS transmits emergency messages, allocation of "emergency indication" to differentiate it from normal CBS messages.	GR_TSTP_3.19_A9
4	IP Multimedia Sub-system (IMS) The IP Multimedia Subsystem (IMS) is a standardized Next Generation Network (NGN) architecture for enabling a mobile to use mobile and fixed multimedia services. IMS uses a number of Internet Protocol (IP)-based services viz. Voice over IP (VoIP), multi-party gaming, video-conferencing, Instant Messaging, community services, presence information and content sharing etc. based on standardized Session Initiation	GR_TSTP_4

	Protocol (SIP) implemented by 3rd Generation Partnership Project (3GPP). SIP is used for the realtime, peer-to-peer, multi-party and multi-media capabilities of IMS. Service control, security functions, routing, registrations, charging, SIP compression and QoS support may be achieved through necessary IMS capabilities The Small Size 5G Core System may have: (I) IMS functionality for supporting SMS. (II) IMS functionality for Voice and Video Service over 5G Network. (III) SIP & RTP interface for external interface towards IP PABX/ MGW for voice interworking etc.	
5	OMC / EMS requirements The OMC allows centralized operation of the various units in the system and functions needed to maintain the sub-systems. The OMC provides the dynamic monitoring and controlling of the network management	Informational
5.1	Management Functions The following management functions shall be carried out through the corresponding OMCs:	Informational
5.1.a	Configuration management	GR_TSTP_5.1_A
5.1.b	Fault report and alarm handling	GR_TSTP_5.1_B
5.1.c	Performance supervision/management	GR_TSTP_5.1_C
5.1.d	Storage of system software and data	GR_TSTP_5.1_D
5.1.e	Security management	GR_TSTP_5.1_E
5.2	OMC database	Informational
5.2.a	The OMC shall use the relational/object-oriented database to store and hold the necessary information for the parameters used in the OMC	GR_TSTP_5.2_A
5.2.b	The OMC database shall include configuration data, maintenance data, fault data and performance / QoS data	GR_TSTP_5.2_B
5.2.c	The database in the OMC shall reside in a disk with mirroring capability	GR_TSTP_5.2_C
5.2.d	The OMC shall be capable of storage of the generated performance data. The methods and capacity of storage provided with the system shall be stated	GR_TSTP_5.2_D
5.2.e	Provision shall be available for collection of statistical information relating to events in the network. Collection frequency shall be configurable	GR_TSTP_5.2_E

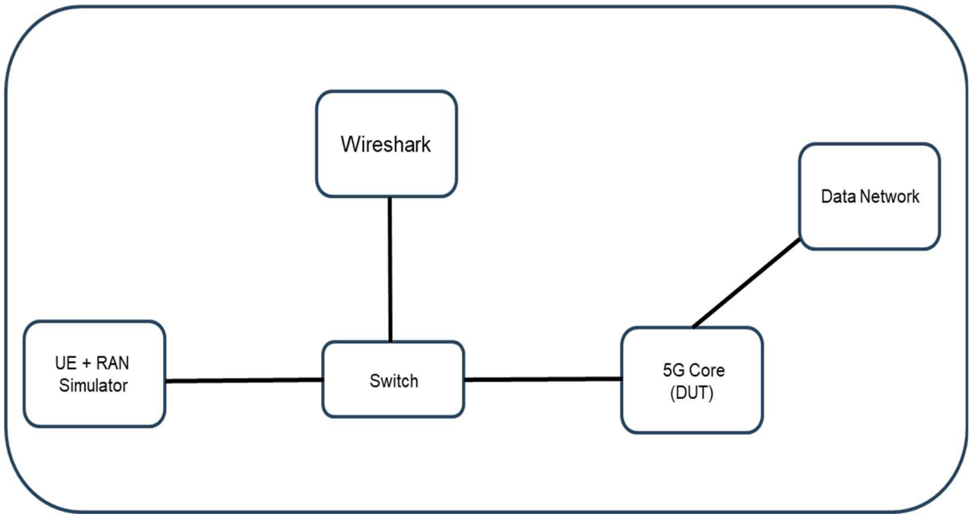
5.2.f	The OMC database shall contain the fault history of the whole network under its command. As a minimum, it shall be possible to search and display data according to the following criteria: Network elements, Severity class, Event type	GR_TSTP_5.2_F
5.3	OMC Generic Features	Informational
5.3.a	OMC software – UNIX/LINUX/Windows System Platform	GR_TSTP_5.3_A
5.3.b	It shall optionally support interface like CORBA / TCP / IP / CMIP / SNMP/ REST / HTTP etc., to enable it to work with a remote NMS.	GR_TSTP_5.3_B
5.3.d	Support Ethernet connectivity with remote network elements	GR_TSTP_5.3_D
5.3.e	Graphical User Interface (GUI). [Alternate text: Management through Element Management System]	GR_TSTP_5.3_E
5.3.f	On-Line Help	GR_TSTP_5.3_F
5.3.g	Consistency Checks	GR_TSTP_5.3_G
5.3.h	Configuration Change/Event Log	GR_TSTP_5.3_G
5.3.i	Object Alarm Status Management / Display	GR_TSTP_5.3_G
5.3.j	Collection of PM counters	GR_TSTP_5.3_G
5.3.k	Limited Access Restriction by User	GR_TSTP_5.3_K
5.3.l	Access Restriction by Function and by Operation	GR_TSTP_5.3_K
6	Generic Common Requirements	Informational
6.1	Operation & Maintenance This section identifies generic O&M requirements to be implemented by the network functions	Informational
6.1.a	The NFs shall provide a flexible & secure management interface for configuration, fault management and performance management	GR_TSTP_6.1_A
6.1.b	The NFs shall include an O&M interface for debugging and troubleshooting	GR_TSTP_6.1_A
6.1.c	NFs shall support at least one of the following interfaces towards EMS	Informational
6.1.c.I	SNMP ~~(Is it required for 5G?)~~	GR_TSTP_6.1_A
6.1.c.II	REST	GR_TSTP_6.1_A
6.1.c.III	HTTPS	GR_TSTP_6.1_A

6.1.d	For performance management, the node shall generate various performance counters and provide mechanism to transfer the same to external entity for further analysis	GR_TSTP_6.1_D
6.1.e	Fault Report and Alarm Handling	GR_TSTP_6.1_E
6.1.e.I	For fault management, the NFs shall support Event Based Monitoring where all events will be streamed out of the NF and available for external processing	GR_TSTP_6.1_E
6.1.e.II	Fault Management system shall have the ability to detect and mitigate or recover from faults	GR_TSTP_6.1_E
6.1.f	Alarm Surveillance Alarms shall be raised for adverse events in the network. The information included in the alarms shall be detailed enough to TEC Standard No. 22160:2023 59 identify which system component is experiencing the failure condition. The detail shall Include	GR_TSTP_6.1_E
6.1.f.I	Alarm type	GR_TSTP_6.1_E
6.1.f.II	The probable cause	GR_TSTP_6.1_E
6.1.f.III	The specific problem	GR_TSTP_6.1_E
6.1.f.IV	The perceived severity	GR_TSTP_6.1_E
6.1.f.V	Network Element ID	GR_TSTP_6.1_E
6.1.f.VI	Network Element Type	GR_TSTP_6.1_E
6.1.g	The alarms shall be automatically cleared when the failure condition is resolved. It shall not record or forward duplicate alarms for detection of the same failure condition	GR_TSTP_6.1_G
6.1.h	The NF shall support software upgrade	GR_TSTP_6.1_H
6.1.k	The control software shall be responsible for logging and sending the log file on the network to a designated syslog server	GR_TSTP_6.1_H
6.1.l	The system shall maintain a system log and core dump logs	GR_TSTP_6.1_L
6.1.m	The NF shall support alarms, events to OMC for visual indicators of status and fault	GR_TSTP_6.1_M
6.1.n	The NF shall have reboot and shut-down capability	GR_TSTP_6.1_N
6.1.o	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)	GR_TSTP_6.1_O

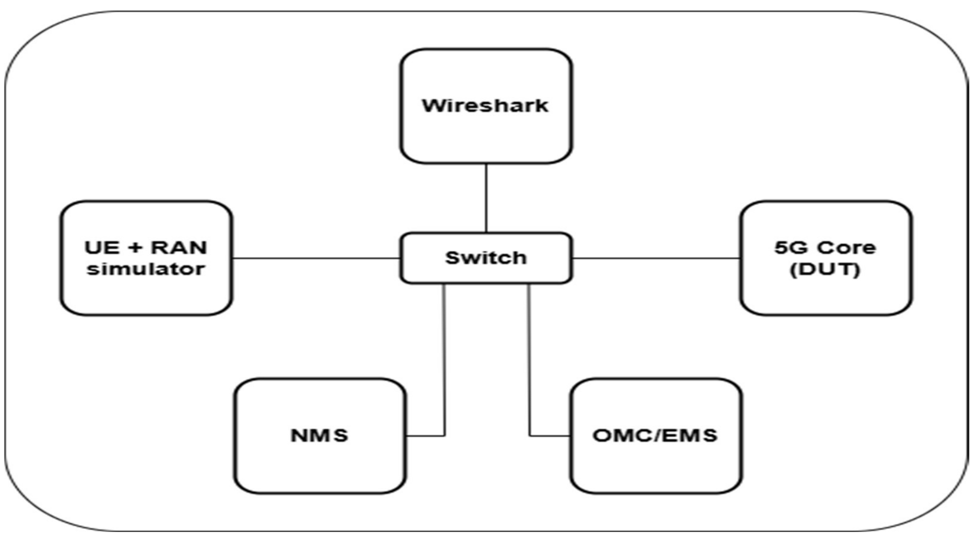
7	General Requirements	Informational
7.1	Software Requirements	Informational
7.1.a	Modular, structured software written in High-Level Language	
7.1.b	Software easy to handle during installation and normal operations as well as during extensions	
7.1.c	Introduction of changes in software, wherever necessary, with least impact on other modules	
7.1.d	Open-ended to allow addition of new features	
7.1.e	Adequate flexibility to easily adopt changes in service features & facilities and technological evolution in hardware	
7.1.f	Propagation of software faults is contained	
7.1.g	Test programs to include fault tracing for detection and localization of system faults	
7.2	Software Maintenance Requirements	
7.2.a	Continuous supply of all software updates, for the period specified	
7.2.b	Integration of software updates without posing any problem to the existing functionality	
8	INFORMATION FOR THE PROCURER OF PRODUCT Interfaces and features which are optional needs to be examined by the procurer and suitably specified in the tender conditions as per their requirement based on the deployment scenario specific to the procurer and mentioned in the following tabular format and these will be used for type approval.	

1. Test Setups:

<u>TEST SETUP Small size 5G Core-1</u>



<u>TEST SETUP Small size 5G Core-2</u>



I. Test Setup & Procedures:

1.Test No	GR_TSTP_3.1.1_A
2. Test Details	To verify that the AMF can successfully connect with AUSF, NG-RAN, SMF, and UDM as per 3GPP specifications.
3. Test Instruments Required	Wireshark, UE + gNB simulator tool
4. Test Setup	Test Setup Small size 5G Core 1
5. Test Procedure	Action: • UE + gNB simulator tool should be running • Enter the IP address of the AMF in the UE + gNB simulator tool • All the core nodes (i.e., SMF, UDM, AUSF) should be running • Initiate the registration and PDU session procedures through UE+ gNB simulator tool Response: • Core has performed the initiated procedures
6. Test Limits	NA
7. Expected Results	AMF should communicate with all the nodes (UE + gNB simulator tool, SMF, UDM, AUSF) Core should perform the initiated procedures.

1.Test No	GR_TSTP_3.1.1_B1
2. Test Details	To verify that the AMF supports primary authentication with AUSF using SUCI and SUPI for 5G AKA over the Service-Based Interface (SBI).
3. Test Instruments Required	Wireshark, UE + gNB simulator tool
4. Test Setup	Test Setup Small size 5G Core-1
5. Test Procedure	Action: • Establish NG setup between AMF and gNB. • Initiate the UE registration procedures by the UE + gNB simulator tool Response: • Primary authentication has been completed with AUSF using SUCI and SUPI for 5G AKA with SBI
6. Test Limits	NA
7. Expected Results	Primary authentication should be completed with AUSF using SUCI and SUPI for 5G AKA with SBI

1.Test No	GR_TSTP_3.1.1_B2
2. Test Details	To verify that the AMF supports at least one 3GPP-based option for control plane signaling confidentiality and integrity protection of NAS signaling.
3. Test Instruments Required	Wireshark, UE + gNB simulator tool
4. Test Setup	Test Setup Small size 5G Core-1
5. Test Procedure	Action: • Initiate UE registration with AMF using N1 NAS interface and verify NAS Security Mode Command. Response: • Ensure the NAS signaling is encrypted and integrity-protected with at least one 3GPP-defined algorithm (e.g., 128-NEA1, 128-NIA1).
6. Test Limits	NA
7. Expected Results	AMF should successfully establish secure NAS signaling, confirm selected encryption/integrity algorithms, and process subsequent NAS messages without failure.

1.Test No	GR_TSTP_3.1.1_B3
2. Test Details	To verify that the AMF correctly handles the UE-initiated PDU session release procedure while in the connected state.
3. Test Instruments Required	Wireshark, UE + gNB simulator tool
4. Test Setup	Test Setup Small size 5G Core-1
5. Test Procedure	Action: • Establish NG setup between AMF and gNB. • Register the UE with 5G core • Establish the PDU session • Initiate the PDU session release procedures through UE + gNB simulator Response: • UE has initiated the PDU session release procedure in the connected state
6. Test Limits	NA
7. Expected Results	UE should initiate the PDU session release procedure in the connected state

1.Test No	GR_TSTP_3.1.1_B4
2. Test Details	To verify that the AMF correctly processes a UE-triggered service request procedure and responds with a service accept message.
3. Test Instruments Required	Wireshark, UE + gNB simulator tool
4. Test Setup	Test Setup Small size 5G Core-1
5. Test Procedure	Action: • Establish NG setup between AMF and gNB. • Register the UE with 5G core • The UE is registered and connected to the network Response: • UE Successfully Initiates Service Request • The UE Successfully sends a Service Request message to the network • The network Successfully sends a Service Request Response message to the UE.
6. Test Limits	NA
7. Expected Results	The AMF receives the message and processes the requested service type and network responds with a Service Request Response message confirming the reception of the request.

1.Test No	GR_TSTP_3.1.1_C1
2. Test Details	Network initiated PDU session release procedure when the UE is in idle state;
3. Test Instruments Required	Wireshark, UE + gNB simulator tool
4. Test Setup	Test Setup Small size 5G Core-1
5. Test Procedure	Action: • Establish NG setup between AMF and gNB. • Register the UE with 5G core • Establish the PDU session • Initiate the PDU session release procedures by the AMF with the curl • Response: • Network has initiated the PDU session release procedure because UE is in idle state.
6. Test Limits	NA
7. Expected Results	The AMF receives the message and processes the requested service type and network responds with a Service Request Response message confirming the reception of the request.

1.Test No	GR_TSTP_3.1.1_C2
2. Test Details	Rejecting PDU session establishment based on SUPI and DNN
3. Test Instruments Required	Wireshark, UE + gNB simulator tool
4. Test Setup	Test Setup Small size 5G Core-1
5. Test Procedure	Action: • Establish NG setup between AMF and gNB. • Initiate the UE registration and PDU session procedures by the UE + gNB simulator tool Response: • Core has rejected the PDU session establishment procedures because of an unknown DNN
6. Test Limits	NA
7. Expected Results	Core should reject the PDU session establishment procedures for unknown DNN

1.Test No	GR_TSTP_3.1.1_C3
2. Test Details	The AMF may provide the SMF with the PEI (Permanent Equipment Identifier) of the UE if the PEI is available with the AMF at the time of PDU session establishment
3. Test Instruments Required	Wireshark, UE + gNB simulator tool
4. Test Setup	Test Setup Small size 5G Core-1
5. Test Procedure	Action: • Establish NG setup between AMF and gNB. • Register the UE with 5G core. • AMF, SMF, and other relevant network elements are operational and configured. • The PEI of the UE is available with the AMF Response: • The PEI to the SMF during PDU session establishment in a 5G network involves a series of messages and procedures between the AMF, SMF, and the UE.
6. Test Limits	NA
7. Expected Results	The SMF successfully receives the UE's PEI information from the AMF during the PDU session establishment. The PDU session is successfully established between the UE and the network

1.Test No	GR_TSTP_3.1.1_C4
2. Test Details	To verify that the AMF may support One CBCF or multiple CBCFs to provide PWS.
3. Test Instruments Required	Wireshark, UE + gNB simulator tool
4. Test Setup	Test Setup Small size 5G Core-1
5. Test Procedure	**Action** • Establish NG setup between AMF and gNB. • Register UE with 5G Core. • Configure one or more CBCFs registered via NRF. • CBCF sends Write-Replace Warning Request to AMF (as per TS 23.041). • AMF forwards request to gNB(s) for broadcasting. **Response** (a) **Single CBCF:** • AMF → gNB: Write-Replace Warning Request • gNB → UE: Broadcast Warning Message (b) **Multiple CBCFs:** • AMF handles multiple CBCF requests without duplication. • Each CBCF's message delivered correctly via gNB.
6. Test Limits	NA
7. Expected Results	(a) For **Single CBCF:** • PWS message successfully broadcast to UE(s). • Correct signaling between CBCF ↔ AMF ↔ gNB observed. (b) For **Multiple CBCFs:** • All CBCFs can independently send PWS messages via AMF. • No duplication or interference between broadcasts. • Proper acknowledgment and message delivery confirmed in logs/Wireshark traces.

1.Test No	GR_TSTP_3.1.1_C5
2. Test Details	Location services for transport for Location Services messages between UE and LMF as well as between RAN and LMF, in case of deployed disaster or temporary networks.
3. Test Instruments Required	Wireshark, UE + gNB simulator tool
4. Test Setup	Test Setup Small size 5G Core-1
5. Test Procedure	**Action:** • Establish NG setup between AMF and gNB (temporary/disaster deployment). • Register UE with 5G Core. • LMF discovery through NRF. • Trigger location service request from UE or AF (Application Function). • AMF forwards location request to LMF via **Namf_Location** service. • LMF exchanges positioning messages with UE through gNB. • Capture signaling between UE–gNB–AMF–LMF using Wireshark. **Response:** • UE ↔ gNB ↔ AMF ↔ LMF message flow established successfully. • LMF receives and processes positioning data. • AMF provides location information response to the requesting entity (AF or UE).
6. Test Limits	NA
7. Expected Results	• Location service transport between UE and LMF, and RAN and LMF, operates correctly even in disaster or temporary network scenarios. • Proper signaling observed for LCS Service Request, Provide Location Information, and Location Response messages. • Accurate location data delivered to requester. • No message loss or routing failure detected in logs/Wireshark traces.

1.Test No	GR_TSTP_3.1.1_C6
2. Test Details	Roaming –Communication with the H-AUSF and H UDM for authentication (N12 interface) and obtaining subscription information (N8 interface).
3. Test Instruments Required	Wireshark, UE + gNB simulator tool
4. Test Setup	Test Setup Small size 5G Core-1
5. Test Procedure	**Action:** • Establish NG setup between AMF and gNB in V-PLMN. • Register the UE in roaming mode (V-PLMN). • AMF in V-PLMN forwards authentication request to **H-AUSF** via **N12** interface. • **H-AUSF** interacts with **H-UDM** via **N8** to obtain authentication vectors. • Authentication response sent back to **V-AMF** through **V-AUSF**. • AMF completes UE registration after successful authentication. • Capture signaling on N12 and N8 interfaces using Wireshark. **Response:** • Successful signaling between **V-AMF ↔ H-AUSF (N12)** and **H-AUSF ↔ H-UDM (N8)**. • Authentication vectors correctly transferred and validated. • UE registration completed in V-PLMN with subscriber information from H-UDM.
6. Test Limits	NA
7. Expected Results	• **N12** and **N8** interfaces operate as defined in **3GPP TS 23.501**. • V-PLMN successfully communicates with H-PLMN for authentication and subscriber data retrieval. • Authentication response and subscription data are correctly exchanged and verified. • UE registration completes successfully in roaming scenario. • Wireshark trace confirms message exchange: • *Nausf_UEAuthentication Authenticate Request/Response* • *Nudm_SubscriberData Management Request/Response*

1.Test No	GR_TSTP_3.1.1_C7
2. Test Details	The AMF may be capable of connecting to: PCF
3. Test Instruments Required	Wireshark, UE + gNB simulator tool
4. Test Setup	Test Setup Small size 5G Core-1
5. Test Procedure	Action: • UE + gNB simulator tool should be running • Enter the IP address of the AMF in the UE + gNB simulator tool • All the core nodes (i.e., SMF, PCF, UDM, AUSF) should be running • Initiate the registration and PDU session procedures through UE+ gNB simulator tool Response: • Core has performed the initiated procedures.
6. Test Limits	NA
7. Expected Results	AMF should communicate with all the nodes (UE + gNB simulator tool, SMF, PCF, UDM, AUSF) Core should perform the initiated procedures.

1.Test No	GR_TSTP_3.2.1_A
2. Test Details	To verify that the SMF can successfully connect with AMF, UPF, and UDM as per 3GPP specifications.
3. Test Instruments Required	Wireshark, UE + gNB simulator tool
4. Test Setup	Test Setup Small size 5G Core-1
5. Test Procedure	Action • Establish NG setup between AMF and gNB • Register the UE with 5G core • PDU establishment Request • Can check PFCP Request/Response • Establish the PDU session Response: • SMF has been performed the PDU session procedures by communicating with AMF, UPF and UDM
6. Test Limits	NA
7. Expected Results	SMF should be capable of connecting to the AMF, UPF, UDM. If PDU session establishment success then SMF has in connected mode with AMF UPF and UDM

1.Test No	GR_TSTP_3.2.1_B
2. Test Details	The SMF shall be capable of connecting to the 1. CHF 2. PCF
3. Test Instruments Required	Wireshark, UE + gNB simulator tool
4. Test Setup	Test Setup Small size 5G Core-1
5. Test Procedure	• Action • • Establish NG setup between AMF and gNB • • Register the UE with 5G core • • PDU establishment Request • • Can check PFCP Request/Response • • Establish the PDU session Response: • SMF has been performed the PDU session procedures by communicating with AMF, UPF, PCF and UDM
6. Test Limits	NA
7. Expected Results	SMF should be capable of connecting to the PCF, CHF If PDU session establishment success then SMF has in connected mode with PCF and CHF

1.Test No	GR_TSTP_3.2.1_C1
2. Test Details	Session establishment between UPF and NG-RAN node;
3. Test Instruments Required	Wireshark, UE + gNB simulator tool
4. Test Setup	UE + gNB simulator tool, AMF, SMF, UPF, UDM, AUSF, UDR, NRF, PCF, NEF, NSSF, BSF
5. Test Procedure	Action • Establish NG setup between AMF and gNB. • Register the UE with 5G core • Establish the PDU session Response: •Session has been established between UPF and NG-RAN • Session has done on N3 Interface
6. Test Limits	NA
7. Expected Results	• Session establishment between UPF and NG-RAN node should be successful • In the user plane, DL-UL data can be transferred.

1.Test No	GR_TSTP_3.2.1_C2
2. Test Details	To verify that the SMF correctly selects and controls the UPF function as per 3GPP specifications.
3. Test Instruments Required	Wireshark, UE + gNB simulator tool
4. Test Setup	Test Setup Small size 5G Core-1
5. Test Procedure	Action • Establish NG setup between AMF and gNB. • Register the UE with 5G core • Establish the PDU session Response: • Selection and control of UPF function are successfully done
6. Test Limits	NA
7. Expected Results	Selection and control of UPF function should happen

1.Test No	GR_TSTP_3.2.1_C3
2. Test Details	To verify that the SMF correctly deletes the UE PDU session upon receiving a request from the AMF with Cause IE set to "REL_DUE_TO_DUPLICATE_SESSION_ID" and optionally for (a) "REL_DUE_TO_SLICE_NOT_AVAILABLE."
3. Test Instruments Required	Wireshark, UE + gNB simulator tool
4. Test Setup	Test Setup Small size 5G Core-1
5. Test Procedure	Action • Establish NG setup between AMF and gNB. • Register the UE with 5G core • Establish the PDU session (a) The cause IE set to "REL_DUE_TO_DUPLICATE_SESSION_ID" from AMF; o When UE Request a New PDU Session Establishment Request with existing PDU ID o Release due to a UE request to establish a new PDU session with an identical PDU session Id o AMF Request Release PDU Session (b) The cause IE set to "REL_DUE_TO_SLICE_NOT_AVAILABLE" from AMF. o Release due to the associated S-NSSAI becomes no longer available Response: (a) The cause IE set to "REL_DUE_TO_DUPLICATE_SESSION_ID" from AMF; o AMF to UE- PDU SESSION RELEASE COMMAND with IE "REL_DUE_TO_DUPLICATE_SESSION_ID" o UE to AMF- PDU SESSION RELEASE COMPLETE (b) The cause IE set to "REL_DUE_TO_SLICE_NOT_AVAILABLE" from AMF.
	o AMF to UE- PDU SESSION RELEASE COMMAND with IE"REL_DUE_TO_SLICE_NOT_AVAILABLE" o UE to AMF- PDU SESSION RELEASE COMPLETE o For the condition time -startT3592 and stop3592
6. Test Limits	NA
7. Expected Results	(a) UE Should release Existing or duplicate PDU Session "REL_DUE_TO_DUPLICATE_SESSION_ID" (b) PDU Session will Released by AMF with IE Cause

	“REL_DUE_TO_SLICE_NOT_AVAILABLE”

1.Test No	GR_TSTP_3.2.1_C4
2. Test Details	To verify that the SMF correctly allocates a static IPv4 address and/or static IPv6 prefix based on subscription information received from the UDM.
3. Test Instruments Required	Wireshark, UE + gNB simulator tool
4. Test Setup	Test Setup Small size 5G Core-1
5. Test Procedure	Action • Establish NG setup between AMF and gNB. • Register the UE with 5G core • Establish the PDU session Response: • PDU session establishment accept with static IP address.
6. Test Limits	NA
7. Expected Results	UE successfully configured static IPv4 address or IPv6 prefix address. It depends on UE as requested PDU type.

1.Test No	GR_TSTP_3.2.1_D1
2. Test Details	UE IP address allocation and management;
3. Test Instruments Required	Wireshark, UE + gNB simulator tool
4. Test Setup	UE + gNB simulator tool, AMF, SMF, UPF, UDM, AUSF, UDR, NRF, PCF, NEF, NSSF, BSF
5. Test Procedure	Action • Establish NG setup between AMF and gNB. • Register the UE with 5G core • Establish the PDU session Response: • UE IP address allocation has been performed during PDU session establishment procedures
6. Test Limits	NA
7. Expected Results	UE IP address allocation should be done properly.

1.Test No	GR_TSTP_3.2.1_D2
2. Test Details	Both a local and central UPF within a PDU session
3. Test Instruments Required	Wireshark, UE + gNB simulator tool
4. Test Setup	UE + gNB simulator tool, AMF, SMF, UPF, UDM, AUSF, UDR, NRF, PCF, NEF, NSSF, BSF
5. Test Procedure	Action • Establish NG setup between AMF and gNB. • Register the UE with 5G core • Establish the PDU session • SMF controls both the UPF local and central UPF • In 5GC should deploy both the UPF local and central
6. Test Limits	NA
7. Expected Results	PDU session should be established for both the UPF local and central UPF

1.Test No	GR_TSTP_3.2.1_D3
2. Test Details	Converged online and offline charging;
3. Test Instruments Required	Wireshark, UE + gNB simulator tool
4. Test Setup	UE + gNB simulator tool, AMF, SMF, UPF, UDM, AUSF, UDR, NRF, PCF, NEF, NSSF, BSF
5. Test Procedure	Action • Online and offline charging should combine • CHF (Charging function) enables Online and Offline Charging by closely interfacing with NF Consumers • (SMF)CTF generates charging events towards to the CHF for converged online and offline charging processing • The Charging Data Request is issued by the SMF only when conditions that are related to chargeable events are met • The SMF shall support converged online and offline charging • The SMF acts as a Charging Transfer Function (CTF). The CTF generates charging events toward the Charging Function (CHF), which is responsible for generating Charging Data Records (CDRs) Response: • Converged charging (Nchf ConvergedCharging) • Charging data "Request & Response" SMF(CTF) to CHF • Response as per Even Request initiated by CTF(SMF)
6. Test Limits	NA
7. Expected Results	• In Converged charging we can perform some operation so as per the operation CHF (converged charging) should response to NF consumer (CTF- Charging Triggered function) • The Charging Data Request and the Charging Data Response messages are exchanged between the SMF and the CHF based on session-based charging

1.Test No	GR_TSTP_3.2.1_D4
2. Test Details	Charging of PDU session using SBI interface;
3. Test Instruments Required	Wireshark, UE + gNB simulator tool
4. Test Setup	UE + gNB simulator tool, AMF, SMF, UPF, UDM, AUSF, UDR, NRF, PCF, NEF, NSSF, BSF
5. Test Procedure	Action • Establish NG setup between AMF and gNB. • Register the UE with 5G core • Establish the PDU session • The SMF shall support PDU session charging using service-based interface • CTF will send Charging Data Request [Initial] to CHF as per PDU • Converged charging allows the SMF to collect charging information related to data volumes sent to and received by the UE/MS per user per PDU session Response: • CHF will response back to SMF(CTF) with 201 created
6. Test Limits	NA
7. Expected Results	CHF (Charging Function) Should send back response to CTF with 201 created

1.Test No	GR_TSTP_3.2.1_D5
2. Test Details	CHF selection based on the Charging Characteristics or using NRF^2
3. Test Instruments Required	Wireshark, UE + gNB simulator tool
4. Test Setup	UE + gNB simulator tool, AMF, SMF, UPF, UDM, AUSF, UDR, NRF, PCF, NEF, NSSF, BSF
5. Test Procedure	Action • Establish NG setup between AMF and gNB. • Register the UE with 5G core • Establish the PDU session • The NRF will be used by the SMF to discover CHF instance(s), in case no CHF addresses could be identified in the charging characteristics Note: In case UE subscribed charging characteristics are received from the UDM which include CHF addresses, they take precedence over the CHF addresses of the pre-provisioned charging characteristics. Response: • SMF Response back to NRF with CHF address and instances
6. Test Limits	NA
7. Expected Results	CHF Should select for charging characteristic and UE will get CHF address

1.Test No	GR_TSTP_3.2.1_D6
2. Test Details	Sending of Charging Data Request [Termination] when abort request is received from the CHF;
3. Test Instruments Required	Wireshark, UE + gNB simulator tool
4. Test Setup	UE + gNB simulator tool, AMF, SMF, UPF, UDM, AUSF, UDR, NRF, PCF, NEF, NSSF, BSF
5. Test Procedure	Action • Establish NG setup between AMF and gNB. • Register the UE with 5G core • Establish the PDU session • SMF Action Charging Data Request [Termination] Close the counts with time stamps Response: • CHF (Charging function) Response "Charging data request [Termination]" to CTF • Charging data request will be close in CHF • Charging Data Request [Termination] Close the counts with time stamps
6. Test Limits	NA
7. Expected Results	• CHF response with session termination (e.g., Credit Limit Reached, Credit Control Not Applicable), abort request • Charging data request will be close in CHF • Charging Data Request [Termination] Close the counts with time stamps • CHF response with session termination (e.g., Credit Limit Reached, Credit Control Not Applicable), abort request

1.Test No	GR_TSTP_3.2.1_D7
2. Test Details	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;
3. Test Instruments Required	Wireshark, UE + gNB simulator tool
4. Test Setup	UE + gNB simulator tool, AMF, SMF, UPF, UDM, AUSF, UDR, NRF, PCF, NEF, NSSF, BSF
5. Test Procedure	Action • Establish NG setup between AMF and gNB. • Register the UE with 5G core • Establish the PDU session • CHF Should allow to change QoS or enable disable • UE should initiate PDU session for Specific QoS (Not for default QFI) Response: • SMF Action Close the counts and start new counts with time stamps for new QoS
6. Test Limits	NA
7. Expected Results	CHF Response back to CTF(SMF) for new CDR (Charging data Request) update for new QoS Charging Data Request [Update]

1.Test No	GR_TSTP_3.2.1_D8
2. Test Details	Sending of Charging Data Request [Update] and close the count with time stamp on expiry of time limit per PDU session;
3. Test Instruments Required	Wireshark, UE + gNB simulator tool
4. Test Setup	UE + gNB simulator tool, AMF, SMF, UPF, UDM, AUSF, UDR, NRF, PCF, NEF, NSSF, BSF
5. Test Procedure	Action • Establish NG setup between AMF and gNB. • Register the UE with 5G core • Establish the PDU session • Expiry of data time limit per PDU session • SMF(CTF) will send Charging Data Request [Update] to CHF • CHF will perform close the count with time stamp and response back to SMF(CTF) Response: • Charging Data Request [Update]
6. Test Limits	NA
7. Expected Results	SMF will get close count response and CHF close the Counts with time stamps

1.Test No	GR_TSTP_3.2.1_D9
2. Test Details	Sending of Charging Data Request [Update] and close the count with time stamp on expiry of data volume limit per PDU session
3. Test Instruments Required	Wireshark, UE + gNB simulator tool
4. Test Setup	UE + gNB simulator tool, AMF, SMF, UPF, UDM, AUSF, UDR, NRF, PCF, NEF, NSSF, BSF
5. Test Procedure	Action • Establish NG setup between AMF and gNB. • Register the UE with 5G core • Establish the PDU session • Expiry of data volume time limit per PDU session • SMF(CTF) will send Charging Data Request [Update] to CHF • CHF will perform close the count with time stamp and response back to SMF(CTF) Response: • Charging Data Request [Update]
6. Test Limits	NA
7. Expected Results	CHF will close the count with time stamp when data volume limit expires as per Request of SMF(CTF)
1.Test No	GR_TSTP_3.2.1_D10
2. Test Details	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.
3. Test Instruments Required	Wireshark, UE + gNB simulator tool
4. Test Setup	UE + gNB simulator tool, AMF, SMF, UPF, UDM, AUSF, UDR, NRF, PCF, NEF, NSSF, BSF
5. Test Procedure	Action • Establish NG setup between AMF and gNB. • Register the UE with 5G core • Establish the PDU session • UE is in CM-IDLE state Response: • Data will come to UPF • Data Notification UPF to SMF • The SMF needs to setup N3 tunnel to deliver Downlink packet to the UE for a PDU Session and the UE is in CM-IDLE state: Step 3a contains an N2 message and Step 4b (paging) is performed • Namf_Communication_N1N2MessageTransfer • Namf_Communication_N1N2MessageTransferResponse • UP (User plane) re-activation (Connected) • Service Request Procedure

6. Test Limits	NA
7. Expected Results	Downlink data should receive to UE by UPF only with DL Notification

1.Test No	GR_TSTP_3.2.2_A1_1
2. Test Details	To verify that the SMF correctly enforces QoS and policy rules as per the subscription and network policies.
3. Test Instruments Required	Wireshark, UE + gNB simulator tool
4. Test Setup	Test Setup Small size 5G Core-1
5. Test Procedure	Action • Establish NG setup between AMF and gNB. • Register the UE with 5G core • PDU session establishment request & Response UE-5G core Response: • PFCP Req./Res message for QoS Rule • QoS flow is identified by QFI within PDU session • PDU Session establishment Request/Response • 5G Network can provide the UE, one or more QoS flow descriptions associated with a PDU session during the PDU session establishment
6. Test Limits	NA
7. Expected Results	QOS and Policy enforcement are successfully done

1.Test No	GR_TSTP_3.2.2_A1_2
2. Test Details	To verify that the SMF shall support default QoS flows
3. Test Instruments Required	Wireshark, UE + gNB simulator tool
4. Test Setup	Test Setup Small size 5G Core-1
5. Test Procedure	**Action:** • Establish NG setup between AMF and gNB. • Register UE and request PDU session establishment (IPv4/IPv6/IPv4v6 as applicable). • SMF queries PCF for QoS policy and receives default QoS flow parameters (5QI/ARP/GBR/non-GBR, QFI mapping). • SMF provisions UPF with default QoS Flow rules (PDR/FAR/QER) via N4. • SMF signals default QoS flow parameters to UE via AMF in PDU Session Establishment Accept. • Generate traffic and observe enforcement at UPF/gNB. • Capture signaling and user-plane using Wireshark. **Response:** • SMF provisions default QoS flow in UPF and signals it to UE/RAN. • UPF enforces QoS per default flow rules. • UE receives default QoS parameters in session accept.
6. Test Limits	NA
7. Expected Results	• SMF creates and maintains a **single default QoS Flow** for the PDU session and applies the parameters received from PCF. • UPF enforces the default QoS Flow (packet handling, GBR/Non-GBR behavior) as provisioned. • UE receives default QoS parameters in PDU Session Establishment Accept. • Signaling traces on **N7/N4/N11** confirm correct policy retrieval, provisioning and signaling. • User-plane traffic conforms to default QoS behaviour (throughput/priority) observed in traces and traffic measurements.

1.Test No	GR_TSTP_3.2.2_A2
2. Test Details	To verify that the SMF correctly establishes, manages, and enforces both Default QoS flows and Dedicated QoS flows as per policy and subscription requirements.
3. Test Instruments Required	Wireshark, UE + gNB simulator tool
4. Test Setup	Test Setup Small size 5G Core-1
5. Test Procedure	Action • Establish NG setup between AMF and gNB. • Register the UE with 5G core • Establish the PDU session • Modify the established PDU session Response: • PDU Session Establishment request/Response • PDU session modification Request/Response
6. Test Limits	NA
7. Expected Results	QoS flows should be different in the PDU session and modified PDU session

1.Test No	GR_TSTP_3.2.2_A3
2. Test Details	To verify that the SMF supports and enforces 5QI values associated with enhanced Mobile Broadband (eMBB) services as per 3GPP specifications.
3. Test Instruments Required	Wireshark, UE + gNB simulator tool
4. Test Setup	Test Setup Small size 5G Core-1
5. Test Procedure	Action • Establish NG setup between AMF and gNB. • Register the UE with 5G core • Establish the PDU session • In PDU session request, if dynamic flag is false then SMF will allocate QFI static • SMF assign default 5QI = 1-254 Response: • SMF has been assigned default 5QI value range from 1-254 according to the dynamic flag in the PDU session request
6. Test Limits	NA
7. Expected Results	When UE send PDU session request SMF If dynamic flag is false then SMF should allocate QFI static SMF assign default 5QI = 67

1.Test No	GR_TSTP_3.2.2_A4
2. Test Details	To verify that the SMF supports a minimum of one QoS flow per UE and optionally up to 16 QoS flows per UE as per 3GPP specifications.
3. Test Instruments Required	Wireshark, UE + gNB simulator tool
4. Test Setup	Test Setup Small size 5G Core-1
5. Test Procedure	Action • Establish NG setup between AMF and gNB. • Register the UE with 5G core • Establish 16 QoS flows for UE across multiple PDU sessions. Response: • PCF will create up to 16 5QI
6. Test Limits	NA
7. Expected Results	UE will configure 16 QoS 5QI as per UE requested services

1.Test No	GR_TSTP_3.2.2_A5
2. Test Details	To verify that the SMF includes Guaranteed Bit Rate (GBR) Flow Bit Rate (GFBR) and Maximum Flow Bit Rate (MFBR) in the QoS profile for each GBR QoS flow as per 3GPP specifications.
3. Test Instruments Required	Wireshark, UE + gNB simulator tool
4. Test Setup	Test Setup Small size 5G Core-1
5. Test Procedure	Action • Establish NG setup between AMF and gNB. • Register the UE with 5G core • Establish the PDU session • Need to enabled GFBR & MFBR in PCF Response: • PDU session establishment Response • In QoS Profile will add GFBR (Guaranteed flow bit rate) & MFBR (Maximum flow bit rate) for both DL-UL
6. Test Limits	NA
7. Expected Results	MFBR should be included in the QoS flow with GBFR MFBR and GBFR info. can see in PDU session accept msg with QOS

1.Test No	GR_TSTP_3.2.2_B1
2. Test Details	QoS handling on Flow level, Service level as well as Session level;
3. Test Instruments Required	Wireshark, UE + gNB simulator tool
4. Test Setup	UE + gNB simulator tool, AMF, SMF, UPF, UDM, AUSF, UDR, NRF, PCF, NEF, NSSF, BSF
5. Test Procedure	Action • Establish NG setup between AMF and gNB. • Register the UE with 5G core • Establish the PDU session
6. Test Limits	NA
7. Expected Results	QoS handling on Flow level, Service level and Session level are successfully performed

1.Test No	GR_TSTP_3.2.2_B2
2. Test Details	Both per-configured and dynamically assigned 5QI
3. Test Instruments Required	Wireshark, UE + gNB simulator tool
4. Test Setup	UE + gNB simulator tool, AMF, SMF, UPF, UDM, AUSF, UDR, NRF, PCF, NEF, NSSF, BSF
5. Test Procedure	Action • Establish NG setup between AMF and gNB. • Register the UE with 5G core • Establish the PDU session • In PDU session request If dynamic flag is true then SMF will allocate QFI Dynamically and If dynamic flag is false then SMF will allocate QFI static Response: • PDU session procedures has been completed according to the flag has set
6. Test Limits	NA
7. Expected Results	PDU session procedures should complete according to the flag has set

1.Test No	GR_TSTP_3.2.2_B3
2. Test Details	operator-specific 5QI in the range of 128-254
3. Test Instruments Required	Wireshark, UE + gNB simulator tool
4. Test Setup	UE + gNB simulator tool, AMF, SMF, UPF, UDM, AUSF, UDR, NRF, PCF, NEF, NSSF, BSF
5. Test Procedure	Action • Establish NG setup between AMF and gNB. • Register the UE with 5G core • Establish the PDU session • configuration need to change in UPF and set operator specific 5QI 128- 254 • Based on the operator policy non-predefined 5QI values can be assigned resulting from the value range of operator specific 5QI (128-254) • Provisioning needs to set operator-specific 5QI in the range of 128-254 Response: • PDU Session establishment request/response • PFCP session establishment Request/Response • SMF has been assigned default 5QI value range from 128-254 according to the dynamic flag in the PDU session request
6. Test Limits	NA
7. Expected Results	UE get successfully 5QI within range of operator specific range 128-254 with "PDU session establishment accept" when UE send PDU session request SMF

1.Test No	GR_TSTP_3.2.2_B4
2. Test Details	Verify that the SMF shall support QCI 65, 66, 69 and 70 - In case of support for MCX services
3. Test Instruments Required	Wireshark, UE + gNB simulator tool
4. Test Setup	Test Setup Small size 5G Core-1
5. Test Procedure	**Action:** • Establish NG setup between AMF and gNB. • Register UE with MCX-enabled subscription profile. • Initiate PDU session for MCX service (e.g., MCPTT, MCVideo, or MCData). • PCF provides QoS policy including QCI 65, 66, 69, or 70 to SMF. • SMF establishes session with corresponding QCI. • Capture PDU session establishment and QoS signaling using Wireshark. **Response:** • SMF requests QoS policy from PCF. • PCF returns correct QCI parameters as per MCX service type. • SMF applies QoS rule and includes QCI in session setup. • gNB applies radio bearer configuration accordingly.
6. Test Limits	NA
7. Expected Results	• SMF correctly supports and applies **QCI 65, 66, 69, and 70** for MCX services. • QCI mapping and QoS parameters verified in Wireshark traces and SMF logs. • PDU session successfully established with assigned QCI value. • Consistent QoS maintained for MCPTT/MCVideo/MCData flows as per **3GPP TS 23.501, Table 5.7.4-1** and **TS 23.203**.

1.Test No	GR_TSTP_3.2.2_B5
2. Test Details	Verify Appropriate QCI values for URLLC use cases, depending on procurer requirement based on deployment scenario
3. Test Instruments Required	Wireshark, UE + gNB simulator tool
4. Test Setup	Test Setup Small size 5G Core-1
5. Test Procedure	**Action:** • Establish NG setup between AMF and gNB. • Register UE with URLLC subscription. • Initiate PDU session for URLLC service (e.g., industrial automation or remote control). • PCF provides QoS policy containing appropriate QCI or 5QI values as per scenario. • SMF applies QoS rule and establishes bearer with corresponding latency and reliability profile. • Capture QoS signaling using Wireshark and verify QCI/5QI assignment. **Response:** • SMF requests QoS information from PCF. • PCF returns suitable QCI/5QI parameters for URLLC. • SMF applies QoS attributes (e.g., packet delay budget < 10 ms, high priority). • gNB configures bearer and confirms activation.
6. Test Limits	NA
7. Expected Results	• Appropriate QCI or 5QI values for URLLC are selected based on deployment and service type. • End-to-end QoS verified — low latency, high reliability. • Correct signaling between SMF ↔ PCF ↔ gNB observed in traces. • PDU session meets URLLC KPIs (latency and reliability) as per 3GPP TS 23.501, Table 5.7.4-1.

1.Test No	GR_TSTP_3.2.2_B6
2. Test Details	Verify Appropriate QCI values for mMTC use cases, depending on procurer requirement based on deployment scenario
3. Test Instruments Required	Wireshark, UE + gNB simulator tool
4. Test Setup	Test Setup Small size 5G Core-1
5. Test Procedure	**Action:** • Establish NG setup between AMF and gNB. • Register multiple mMTC UEs with 5G Core. • Initiate PDU sessions for mMTC-type data transfer. • PCF provides QoS policy with appropriate QCI/5QI based on service type (e.g., sensor telemetry, periodic reporting). • SMF applies the QoS policy and establishes session accordingly. • Capture QoS signaling using Wireshark to verify assigned QCI/5QI. **Response:** • SMF requests and applies low-priority QoS rules from PCF. • PCF returns QCI/5QI parameters optimized for mMTC traffic (low data rate, high delay tolerance). • gNB configures bearer parameters accordingly.
6. Test Limits	NA
7. Expected Results	• Appropriate QCI or 5QI values assigned for mMTC use cases depending on deployment (e.g., smart metering, IoT sensors). • PDU sessions established successfully with corresponding QoS characteristics — low bandwidth, non-delay sensitive. • Correct signaling between SMF ↔ PCF ↔ gNB observed in Wireshark traces. • End-to-end QoS performance matches 3GPP TS 23.501 Table 5.7.4-1 for mMTC profiles.

1.Test No	GR_TSTP_3.2.2_B7
2. Test Details	The SMF may support packet marking for HTTP/2 signaling over SBI
3. Test Instruments Required	Wireshark, UE + gNB simulator tool
4. Test Setup	UE + gNB simulator tool, AMF, SMF, UPF, UDM, AUSF, UDR, NRF, PCF, NEF, NSSF, BSF
5. Test Procedure	Action • Establish NG setup between AMF and gNB. • Register the UE with 5G core • Establish the PDU session • HTTP/2 should be enabled in 5GC • Control signaling should happened with HTTP/2 between Nfs • All network entities communicate each other by using HTTP/2 • The SMF can change the transport-level marking by the change of the Transport Level Marking IE in the related FAR Response: • The SMF controls the transport-level marking and provides the DSCP in the Type of service (IPv4) or Traffic Class (IPv6) within the Transport Level Marking Information Element (IE) in the Forward AC=Action Rule (FAR), which is associated with the PDR that matches the traffic to be marked
6. Test Limits	NA
7. Expected Results	Need to check PCFP establishment request to check as per response massages, as per 3GPP not sure about the SMF packet marking (FAR Value needs to check)

1.Test No	GR_TSTP_3.3.1_A
2. Test Details	To verify that the UPF can successfully connect with the SMF, NG-RAN, and Data Network as per 3GPP specifications.
3. Test Instruments Required	Wireshark, UE + gNB simulator tool
4. Test Setup	Test Setup Small size 5G Core-1
5. Test Procedure	Action • Establish NG setup between AMF and gNB. • Register the UE with 5G core • Establish a PDU session with PDR, QER, BAR, FAR and provisioning that at UPF. • Running the uplink and downlink data. Response: • UPF has apply the provision requested parameter.
6. Test Limits	NA
7. Expected Results	UPF should apply the parameter by SMF and also forward data according that rules.

1.Test No	GR_TSTP_3.3.1_B1
2. Test Details	To verify that the UPF correctly detects packets based on predefined PDRs or PDRs received via PFCP messages from the SMF over the N4 interface.
3. Test Instruments Required	Wireshark, UE + gNB simulator tool
4. Test Setup	Test Setup Small size 5G Core-1
5. Test Procedure	Action • Establish NG setup between AMF and gNB. • Register the UE with 5G core • Establish a PDU session with the PDR's. • SMF will send PFCP session establishment request to the UPF with the PDR's. Response: • UPF stores the received PDRs in the PFCP session establishment request and UPF passes the data based on the received PDR's.
6. Test Limits	NA
7. Expected Results	UPF should store the received PDRs in the PFCP session establishment request and it should pass the data based on the received PDR's.

1.Test No	GR_TSTP_3.3.1_B2
2. Test Details	To verify that the UPF successfully establishes and manages a PDU session carrying IPv4 traffic as per 3GPP specifications.
3. Test Instruments Required	Wireshark, UE + gNB simulator tool
4. Test Setup	Test Setup Small size 5G Core-1
5. Test Procedure	Action • Establish NG setup between AMF and gNB. • Register the UE with 5G core • Establish a PDU session which can support IPv4 ~~or IPv6~~ traffic. Response: • PDU session have carried IPv4 ~~or IPv6~~ traffic.
6. Test Limits	NA
7. Expected Results	PDU session should carry the IPv4 ~~or IPv6~~ traffic.

1.Test No	GR_TSTP_3.3.1_B3
2. Test Details	To verify that the UPF correctly uses the QoS Flow ID (QFI) to identify and manage QoS flows as per 3GPP specifications.
3. Test Instruments Required	Wireshark, UE + gNB simulator tool
4. Test Setup	Test Setup Small size 5G Core-1
5. Test Procedure	Action • Establish NG setup between AMF and gNB. • Register the UE with 5G core • Establish a PDU session. • During the PDU session establishment, SMF sends a PFCP session establishment request with the QFI parameter to UPF. Response: • UPF has identified the QoS flow based on the received QFI and passed the data traffic through the QoS flow.
6. Test Limits	NA
7. Expected Results	UPF should identify the QoS flow based on the received QFI and it should pass the data traffic through the QoS flow.

1.Test No	GR_TSTP_3.3.1_B4
2. Test Details	To verify that the UPF correctly maps user plane traffic to QoS flows based on Service Data Flow (SDF) templates as per 3GPP specifications.
3. Test Instruments Required	Wireshark, UE + gNB simulator tool
4. Test Setup	Test Setup Small size 5G Core-1
5. Test Procedure	Action • Establish NG setup between AMF and gNB. • Register the UE with 5G core • Establish a PDU session. • During the PDU session establishment, SMF sends a PFCP session establishment request with the information related to QoS, including the SDF templates. Response: • When user data traffic arrives at the UPF, the UPF examines the traffic characteristics and applies the appropriate SDF Template. This involves matching the traffic against the packet filters defined in the SDF templates. Once a match is found, the UPF applies the corresponding QoS parameters and traffic handling rules to ensure that the traffic receives the desired treatment.
6. Test Limits	NA
7. Expected Results	UPF should categorize incoming user data flows into specific service data flows based on predefined templates and then apply QoS and traffic handling rules accordingly.

1.Test No	GR_TSTP_3.3.1_C1
2. Test Details	Buffering of packets instead of immediately forwarding them based on the instructions received from the control plane;
3. Test Instruments Required	Wireshark, UE + gNB simulator tool
4. Test Setup	UE + gNB simulator tool, AMF, SMF, UPF, UDM, AUSF, UDR, NRF, PCF, NEF, NSSF, BSF
5. Test Procedure	Action • Establish NG setup between AMF and gNB. • Register the UE with 5G core • Establish a PDU session. • During the PDU session establishment, SMF sends a PFCP session establishment request with the information related to QoS, including the SDF templates. Response: UPF has buffered the packets instead of immediately forwarding them based on the instructions received from the control plane.
6. Test Limits	NA
7. Expected Results	UPF should buffer the packets instead of immediately forwarding them based on the instructions received from the control plane.

1.Test No	GR_TSTP_3.3.1_C2
2. Test Details	Downlink Data Notification functionality;
3. Test Instruments Required	Wireshark, UE + gNB simulator tool
4. Test Setup	UE + gNB simulator tool, AMF, SMF, UPF, UDM, AUSF, UDR, NRF, PCF, NEF, NSSF, BSF
5. Test Procedure	Action • Establish NG setup between AMF and gNB. • Register the UE with 5G core • Establish a PDU session. • When UE turns to ECM-Idle state • • DDN functionality should enables in SMF. Response: • SMF Should sends Sx_Modify_Request with FAR Apply action set to buffer value to AMF • When UE is active, Sx_Modify_Request reaches UPF with FAR Apply Action set to FWD (Forward) and TEID (Tunnel Endpoint Identifier).
6. Test Limits	NA
7. Expected Results	• SMF and UPF should send response msg. as above • When UE is active then UE should receive buffer packets • When UE will come in active state UPF debuffers the packets and sends them to UE as FIFO. For each packet, rule match will take place after the debuffering process..

1.Test No	GR_TSTP_3.3.1_C3
2. Test Details	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. Test Instruments Required	Wireshark, UE + gNB simulator tool
4. Test Setup	UE + gNB simulator tool, AMF, SMF, UPF, UDM, AUSF, UDR, NRF, PCF, NEF, NSSF, BSF
5. Test Procedure	Action • Establish NG setup between AMF and gNB. • Register the UE with 5G core • Establish a PDU session. • During the PDU session establishment, SMF sends a URR to the UPF. The URR includes information about the committed QoS parameters. • Run the Uplink and Downlink data. Response: • The User Plane Function (UPF) monitors the downlink traffic for the specific user or session and dropped the downlink traffic after the traffic exceeds the reserved resources and sent a report to the SMF
6. Test Limits	NA
7. Expected Results	UPF should drop the downlink traffic and it send report to the SMF if traffic exceeds the received URR threshold.

1.Test No	GR_TSTP_3.3.1_C4
2. Test Details	Verify User Traffic Redirection based on Destination IP
3. Test Instruments Required	Wireshark, UE + gNB simulator tool
4. Test Setup	UE + gNB simulator tool, AMF, SMF, UPF, UDM, AUSF, UDR, NRF, PCF, NEF, NSSF, BSF
5. Test Procedure	**Action:** • Establish NG setup between AMF and gNB. • Register UE and establish PDU session. • Generate traffic from UE targeting specific destination IPs. • SMF applies traffic redirection rules for the corresponding destination IP. • Verify that redirected traffic is sent to the configured target gateway/server. • Capture packet flow and signaling using Wireshark for verification. **Response:** • Traffic from UE with matched destination IP is redirected by SMF to configured target. • UE traffic for non-matching IPs continues normal path. • Correct signaling and policy enforcement observed in SMF and PCF logs.
6. Test Limits	NA
7. Expected Results	• SMF correctly redirects user traffic based on destination IP. • Traffic reaches the intended target without loss or duplication. • Wireshark traces confirm redirected traffic and policy application. • Signaling between SMF ↔ UPF ↔ gNB reflects the applied redirection rules.

1.Test No	GR_TSTP_3.3.1_C5
2. Test Details	Verify PDU session that carries Ipv6 traffic.
3. Test Instruments Required	Wireshark, UE + gNB simulator tool
4. Test Setup	UE + gNB simulator tool, AMF, SMF, UPF, UDM, AUSF, UDR, NRF, PCF, NEF, NSSF, BSF
5. Test Procedure	**Action:** • Establish NG setup between AMF and gNB. • Register UE with 5G Core. • UE requests **PDU session** with IPv6 type. • SMF allocates IPv6 address to UE. • UPF forwards IPv6 traffic between UE and DN. • Capture signaling and user plane packets using Wireshark. **Response:** • AMF/SMF establishes PDU session with IPv6. • UE receives valid IPv6 address. • IPv6 traffic successfully exchanged between UE and DN. • Correct signaling observed between **UE ↔ gNB ↔ UPF ↔ DN**.
6. Test Limits	NA
7. Expected Results	• PDU session with IPv6 type is successfully established. • IPv6 address allocation to UE is correct. • End-to-end IPv6 traffic flows without packet loss. • Wireshark traces confirm proper PDU session signaling and IPv6 user plane traffic.

1.Test No	GR_TSTP_3.3.1_C6
2. Test Details	The UPF may support: Application detection;
3. Test Instruments Required	Wireshark, UE + gNB simulator tool
4. Test Setup	UE + gNB simulator tool, AMF, SMF, UPF, UDM, AUSF, UDR, NRF, PCF, NEF, NSSF, BSF
5. Test Procedure	Action • Establish NG setup between AMF and gNB. • Register the UE with 5G core • Establish a PDU session. • Run the Uplink and Downlink data. Response: • UPF starts the process of analyzing data packets to determine the type of application or service generating the traffic.
6. Test Limits	NA
7. Expected Results	UPF should analyze data packets to determine the type of application or service generating the traffic.

1.Test No	GR_TSTP_3.3.1_C7
2. Test Details	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;
3. Test Instruments Required	Wireshark, UE + gNB simulator tool
4. Test Setup	UE + gNB simulator tool, AMF, SMF, UPF, UDM, AUSF, UDR, NRF, PCF, NEF, NSSF, BSF
5. Test Procedure	Action • Extract the URL from the HTTP POST request message. • Break down the URL into its individual components, including the scheme (http/https), host, port, path, and fragments. • Normalize the scheme: Ensure that the scheme is lowercase (http or https). • Normalize the host: Convert the host portion of the URL to lowercase to ensure case-insensitivity. • Normalize the port: If a port is specified, ensure it's in the standardized format (e.g., port 80 for http, port 443 for https) and remove it if it matches the default port for the scheme. • Normalize the path: Ensure the path follows a consistent format (e.g., leading slash) Response: • After normalizing each component, reconstructed the normalized URL and classified the HTTP POST request as a standard request after the normalized URL matches a standardized format.
6. Test Limits	NA
7. Expected Results	After normalizing each component, it should reconstruct the normalized URL and should classify the HTTP POST request as a standard request after the normalized URL matches a standardized format.

1.Test No	GR_TSTP_3.3.1_C8
2. Test Details	Tethering detection based on TTL values;
3. Test Instruments Required	Wireshark, UE + gNB simulator tool
4. Test Setup	UE + gNB simulator tool, AMF, SMF, UPF, UDM, AUSF, UDR, NRF, PCF, NEF, NSSF, BSF
5. Test Procedure	Action • Establish NG setup between AMF and gNB. • Register the UE with 5G core • Establish a PDU session. • Run the uplink and downlink data. Response: • UPF has been identified the device which is acting as a hotspot and providing internet connectivity to other devices based on the TTL values received in the data packets.
6. Test Limits	NA
7. Expected Results	UPF should identify the tethered devices based on the TTL values received in the data packets.

1.Test No	GR_TSTP_3.3.1_C9
2. Test Details	Multi-homed PDU session;
3. Test Instruments Required	Wireshark, UE + gNB simulator tool
4. Test Setup	UE + gNB simulator tool, AMF, SMF, UPF, UDM, AUSF, UDR, NRF, PCF, NEF, NSSF, BSF
5. Test Procedure	Action • Establish NG setup between AMF and gNB. • Register the UE with 5G core • Establish a PDU session. • Run the uplink and downlink data. Response: • UPF has been sent and received the data through multiple data network interfaces simultaneously.
6. Test Limits	NA
7. Expected Results	UPF should send and receive the data through multiple data network interfaces simultaneously.

1.Test No	GR_TSTP_3.3.1_C10
2. Test Details	HTTP Pipelining Request-Response matching enabling the user plane to match each HTTP response with the corresponding HTTP request;
3. Test Instruments Required	Wireshark, UE + gNB simulator tool
4. Test Setup	UE + gNB simulator tool, AMF, SMF, UPF, UDM, AUSF, UDR, NRF, PCF, NEF, NSSF, BSF
5. Test Procedure	Action • The client initiates multiple HTTP requests in quick succession over a single network connection without waiting for the responses. • The user plane forwards the pipelined HTTP requests to the server. • The server processes the pipelined requests in the order they were received. It generates responses for each request and sends them back to the client through the user plane. Response: • The user plane, as part of its processing, has ensured that each HTTP response is matched with the correct corresponding HTTP request to achieve this, the user plane has used mechanisms such as sequence numbers or message IDs to associate responses with requests. • It forwarded the response to the client after the user plane matches a response with its corresponding request.
6. Test Limits	NA
7. Expected Results	User plane should process the received responses and it should forward to client.

1.Test No	GR_TSTP_3.3.1_C11
2. Test Details	Service chaining functionality allowing the user plane to steer subscriber traffic to third-party service functions in the N6 or SGi- LAN.
3. Test Instruments Required	Wireshark, UE + gNB simulator tool
4. Test Setup	UE + gNB simulator tool, AMF, SMF, UPF, UDM, AUSF, UDR, NRF, PCF, NEF, NSSF, BSF
5. Test Procedure	Action • Establish NG setup between AMF and gNB. • Register the UE with 5G core • Establish a PDU session. • Run the uplink data and Downlink data. Response: • UPF done the sequential processing of data packets (service chaining functionality) for the packets received from the multiple network functions or services. These network functions could include various services such as firewall, deep packet inspection (DPI), video optimization, encryption, and more.
6. Test Limits	NA
7. Expected Results	UPF should perform the service chaining functionality on the packets received from the network functions.

1.Test No	GR_TSTP_3.3.1_C12
2. Test Details	Sending User Plane Inactivity Report to the SMF as a response when instructed;
3. Test Instruments Required	Wireshark, UE + gNB simulator tool
4. Test Setup	UE + gNB simulator tool, AMF, SMF, UPF, UDM, AUSF, UDR, NRF, PCF, NEF, NSSF, BSF
5. Test Procedure	Action • Establish NG setup between AMF and gNB. • Register the UE with 5G core • Establish a PDU session. • Run the uplink data and Downlink data. Response: • UPF has sent a User Plane Inactivity Report to the SMF after the detection of no data is being transmitted or received for a specific user or session.
6. Test Limits	NA
7. Expected Results	UPF should send User Plane Inactivity report to the SMF if it detects no data is being transmitted or received for a specific user or session.

1.Test No	GR_TSTP_3.3.1_C13
2. Test Details	N4 session level report procedure based on Usage Report;
3. Test Instruments Required	Wireshark, UE + gNB simulator tool
4. Test Setup	UE + gNB simulator tool, AMF, SMF, UPF, UDM, AUSF, UDR, NRF, PCF, NEF, NSSF, BSF
5. Test Procedure	**Action:** • Establish NG setup between AMF and gNB. • Register UE and establish PDU session(s). • Generate user traffic through the UPF. • UPF creates **N4 Session Usage Report** messages according to **TS 29.244**. • UPF sends Usage Reports to SMF via N4 Session Reporting procedures. • Capture N4 signaling and verify report contents using Wireshark. **Response:** • SMF receives session-level Usage Reports from UPF. • Reports include bytes transmitted, session duration, QFI/QCI, and other relevant counters. • SMF processes usage data for monitoring, billing, or policy enforcement.
6. Test Limits	NA
7. Expected Results	• N4 session-level Usage Reports are correctly generated by UPF. • SMF successfully receives and processes all reported metrics. • Reports match actual UE traffic and session attributes. • Wireshark traces confirm correct **N4 session reporting** signaling and content as per **3GPP TS 29.244**.

1.Test No	GR_TSTP_3.3.1_C14
2. Test Details	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. Test Instruments Required	Wireshark, UE + gNB simulator tool
4. Test Setup	UE + gNB simulator tool, AMF, SMF, UPF, UDM, AUSF, UDR, NRF, PCF, NEF, NSSF, BSF
5. Test Procedure	Action • The UPF generates usage reports that provide information about the data usage, resource utilization, and other relevant metrics of a PDU session. • UPF performs the detecting the initiation of traffic within a PDU session. This detection could be based on factors like the first data packet sent or received within the session. • Stop of Traffic detection could be triggered by the absence of data packets for a certain duration, signaling the end of communication for that session. • This step involves monitoring the PDU session for inactivity, where no data packets are exchanged. If the session remains inactive for a specified period, the network may decide to release or deactivate the session to free up resources. Response: • UPF will perform the activities which are mentioned in the action section. Activities can perform according to the situation.
6. Test Limits	NA
7. Expected Results	UPF should perform the activities which are mentioned in the action section.

1.Test No	GR_TSTP_3.3.1_C15
2. Test Details	Verify Roaming- Communication between visited UPF and Home UPF using the N9 interface.
3. Test Instruments Required	Wireshark, UE + gNB simulator tool
4. Test Setup	UE + gNB simulator tool, AMF, SMF, UPF, UDM, AUSF, UDR, NRF, PCF, NEF, NSSF, BSF
5. Test Procedure	**Action:** • Establish NG setup between V-AMF and gNB. • Register UE in roaming mode (V-PLMN). • Establish PDU session that requires user plane traffic to H-DN via H-UPF. • V-UPF forwards UE traffic to H-UPF using **N9 interface**. • Capture N9 user plane packets and signaling using Wireshark. **Response:** • V-UPF correctly forwards traffic to H-UPF over N9. • H-UPF receives traffic and forwards to Home DN. • Correct QoS handling and traffic steering maintained. • N9 interface signaling and user plane observed as per 3GPP specifications.
6. Test Limits	NA
7. Expected Results	• N9 interface successfully carries user plane traffic between V-UPF and H-UPF. • PDU session continuity maintained during roaming. • QoS parameters preserved end-to-end. • Wireshark traces confirm correct traffic forwarding and session handling.

1.Test No	GR_TSTP_3.3.2_A1
2. Test Details	To verify that the UPF supports and manages non-guaranteed flow bit rate (non-GBR) QoS flows as per 3GPP specifications.
3. Test Instruments Required	Wireshark, UE + gNB simulator tool
4. Test Setup	Test Setup Small size 5G Core-1
5. Test Procedure	Action • Establish NG setup between AMF and gNB. • Register the UE with 5G core • Establish a PDU session. • During the establishment of the PDU session, SMF sent a PFCP Session establishment request with the Non-GBR to the UPF. • Run the uplink data. Response: • UPF has sent the data traffic based on the received Non-GBR.
6. Test Limits	NA
7. Expected Results	UPF should sent the data traffic based on the received Non-GBR

1.Test No	GR_TSTP_3.3.2_A2
2. Test Details	To verify that the UPF enforces the PDU Session Aggregate Maximum Bit Rate (AMBR) across all non-GBR QoS flows within a PDU session as per 3GPP specifications.
3. Test Instruments Required	Wireshark, UE + gNB simulator tool
4. Test Setup	Test Setup Small size 5G Core-1
5. Test Procedure	Action • Establish NG setup between AMF and gNB. • Register the UE with 5G core • Establish a PDU session for a non-GBR QoS flows. • AMBR value sent to the UPF by the AMF in PDU Session resource setup response through SMF. • UPF has processed the QoS rules, including the AMBR value, to configure the resources and QoS parameters accordingly. Response: • The UPF responds to the AMF through the SMF. This response confirms the establishment and configuration of resources and includes any modifications made by the UPF, such as updated QoS parameters.
6. Test Limits	NA
7. Expected Results	The UPF should respond to the AMF through the SMF and the response should contain the establishment and configuration of resources and includes any modifications made by the UPF, such as updated QoS parameters.

1.Test No	GR_TSTP_3.3.2_A3
2. Test Details	To verify that the UPF correctly drops packets that exceed the limits defined in any associated QoS Enforcement Rules (QERs) as per 3GPP specifications.
3. Test Instruments Required	Wireshark, UE + gNB simulator tool
4. Test Setup	Test Setup Small size 5G Core-1
5. Test Procedure	Action • A data packet arrives at the UPF for processing and the UPF evaluates the packet against the QERs associated with the PDU session and the relevant QoS flows. • If the packet's characteristics (e.g., size, rate) violate the limits defined by any of the associated QERs, it is considered to be exceeding the QoS parameters. Response: • In response to the packet exceeding QER limits, the UPF enforces the QoS policies and the UPF may take various actions like Dropping the Packet, Marking the Packet etc.
6. Test Limits	NA
7. Expected Results	If any packet exceeds the limits of any of the associated QERs, UPF should drop the packets.

1.Test No	GR_TSTP_3.3.2_B1
2. Test Details	Verify UPF may support the QOS Flow for Guaranteed flow bit rate QoS flows;
3. Test Instruments Required	Wireshark, UE + gNB simulator tool
4. Test Setup	UE + gNB simulator tool, AMF, SMF, UPF, UDM, AUSF, UDR, NRF, PCF, NEF, NSSF, BSF
5. Test Procedure	**Action:** • Establish NG setup between AMF and gNB. • Register UE and establish PDU session with GFBR QoS Flows. • SMF provides QoS rules with GFBR values to UPF. • UE generates traffic matching GFBR flows. • Capture user plane traffic and QoS enforcement via Wireshark. **Response:** • UPF applies GFBR for each QoS Flow as per SMF instructions. • Traffic exceeding GFBR is limited; traffic below GFBR is guaranteed minimum rate. • Correct enforcement confirmed by observed user plane metrics.
6. Test Limits	NA
7. Expected Results	• UPF correctly enforces Guaranteed Flow Bit Rate for QoS Flows. • PDU session traffic adheres to minimum and maximum bit rate parameters. • Signaling and QoS enforcement observed in SMF ↔ UPF ↔ gNB messages. • Wireshark traces confirm GFBR applied per flow as per 3GPP TS 23.501 Table 5.7.4-1.

1.Test No	GR_TSTP_3.3.2_B2
2. Test Details	Transport level packet marking with a DSCP value.
3. Test Instruments Required	Wireshark, UE + gNB simulator tool
4. Test Setup	UE + gNB simulator tool, AMF, SMF, UPF, UDM, AUSF, UDR, NRF, PCF, NEF, NSSF, BSF
5. Test Procedure	Action • Establish NG setup between AMF and gNB. • Register the UE with 5G core • Establish a PDU session. • During the establishment of the PDU session, SMF sent a PFCP Session establishment request with the DSCP value in FAR IE. • Run the uplink data. Response: • Data packets arrived at the UPF for processing and started examine the incoming packets to determine their type, source, destination, or any other relevant attributes. Based on this traffic classification, the UPF assigned an appropriate DSCP value to the packets.
6. Test Limits	NA
7. Expected Results	UPF should assign an appropriate DSCP value to the packets.

1.Test No	GR_TSTP_3.3.2_B3
2. Test Details	The UPF may support inclusion of QFI and an indication for reflective QoS activation in the encapsulation header.
3. Test Instruments Required	Wireshark, UE + gNB simulator tool
4. Test Setup	UE + gNB simulator tool, AMF, SMF, UPF, UDM, AUSF, UDR, NRF, PCF, NEF, NSSF, BSF
5. Test Procedure	Action • When the 5GC determines to use Reflective QoS for a specific SDF, the SMF shall ensure that the UPF applies the RQI marking for this SDF. • The SMF shall also ensure that the uplink packets for this SDF can be received by the UPF from the QoS Flow to which the DL PDR of the SDF is associated with, e.g., by generating a new UL PDR for this SDF for that QoS Flow and providing it to the UPF. Response: • UPF has set the RQI in the encapsulation header on the N3 reference point for every DL packet corresponding to this SDF after SMF instructed to the UPF to apply RQI marking and UPF includes the QFI values to apply appropriate QoS policies to incoming packets.
6. Test Limits	NA
7. Expected Results	UPF should set the RQI and QFI values in the encapsulation header on the N3 reference point for every DL packet corresponding to this SDF

1.Test No	GR_TSTP_3.3.2_B4
2. Test Details	The Reflective QoS Indication (RQI) in the encapsulation header on N3 reference point together with the QFI.
3. Test Instruments Required	Wireshark, UE + gNB simulator tool
4. Test Setup	UE + gNB simulator tool, AMF, SMF, UPF, UDM, AUSF, UDR, NRF, PCF, NEF, NSSF, BSF
5. Test Procedure	Action • When the 5GC determines to use Reflective QoS for a specific SDF, the SMF shall ensure that the UPF applies the RQI marking for this SDF. • The SMF shall also ensure that the uplink packets for this SDF can be received by the UPF from the QoS Flow to which the DL PDR of the SDF is associated with, e.g., by generating a new UL PDR for this SDF for that QoS Flow and providing it to the UPF. Response: • UPF has set the RQI in the encapsulation header on the N3 reference point for every DL packet corresponding to this SDF after SMF instructed to the UPF to apply RQI marking and UPF includes the QFI values to apply appropriate QoS policies to incoming packets.
6. Test Limits	NA
7. Expected Results	UPF should set the RQI and QFI values in the encapsulation header on the N3 reference point for every DL packet corresponding to this SDF

1.Test No	GR_TSTP_3.3.2_B5
2. Test Details	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. Test Instruments Required	Wireshark, UE + gNB simulator tool
4. Test Setup	UE + gNB simulator tool, AMF, SMF, UPF, UDM, AUSF, UDR, NRF, PCF, NEF, NSSF, BSF
5. Test Procedure	Action • Establish NG setup between AMF and gNB. • Register the UE with 5G core • Establish a PDU session. • During the establishment of PDU session, SMF send PFCP session establishment request to the UPF with the parameters QFI and QER. Response: • As packets belonging to a specific QoS flow within a PDU session are processed by the UPF, the UPF marked the PDU session container with the QFI value specified in the corresponding QER and sends PDU session containers over the interfaces N3 and N9. The QFI marking is included in the encapsulation headers of the packets.
6. Test Limits	NA
7. Expected Results	UPF should mark the PDU containers and it should send over the interfaces N3 and N9.

1.Test No	GR_TSTP_3.4.1_A
2. Test Details	To verify that the UDM successfully connects with SMF over N10, AMF over N8, and AUSF over N13 using standard 3GPP interfaces.
3. Test Instruments Required	Wireshark, UE + gNB simulator tool
4. Test Setup	Test Setup Small size 5G Core-1
5. Test Procedure	Action • Establish NG setup between AMF and gNB. • Register the UE with 5G core • Establish the PDU session Response: • UDM has connected with other 3GPP network elements using standard Interfaces
6. Test Limits	NA
7. Expected Results	UDM should communicated with the required nodes while we are performing registration and PDU session procedures

1.Test No	GR_TSTP_3.4.1_B
2. Test Details	UDM may be connected with other 3GPP network elements using standard Interfaces: I). SMSF, N21. II). UDR, N35;
3. Test Instruments Required	Wireshark, UE + gNB simulator tool
4. Test Setup	UE + gNB simulator tool, AMF, SMF, UPF, UDM, AUSF, UDR, NRF, PCF, NEF, NSSF, BSF
5. Test Procedure	Action • Establish NG setup between AMF and gNB. • Register the UE with 5G core • Establish the PDU session Response: • UDM has connected with other 3GPP network elements using standard Interfaces
6. Test Limits	NA
7. Expected Results	UDM should communicated with the required nodes while we are performing registration and PDU session procedures.

1.Test No	GR_TSTP_3.4.1_C1
2. Test Details	To verify that the UDM supports identification and authentication functions as per 3GPP specifications.
3. Test Instruments Required	Wireshark, UE + gNB simulator tool
4. Test Setup	Test Setup Small size 5G Core-1
5. Test Procedure	Action • Establish NG setup between AMF and gNB. • Register the UE with 5G core using SUCI value • Establish the PDU session Response: • UE successfully authenticated and registered in 5G network with slice.
6. Test Limits	NA
7. Expected Results	UDM getting authentication and subscribe slice from UDR based on UE data provision

1.Test No	GR_TSTP_3.4.1_C2
2. Test Details	To verify that the UDM maintains AMF/SMF registration sessions as per 3GPP specifications.
3. Test Instruments Required	Wireshark, UE + gNB simulator tool
4. Test Setup	Test Setup Small size 5G Core-1
5. Test Procedure	Action • Establish NG setup between AMF and gNB. • Register the UE with 5G core • Establish the PDU session Response: • AM and SM data stored in UDM after the UE registration and PDU establishment.
6. Test Limits	NA
7. Expected Results	UDM providing AM and SM data based on provision

1.Test No	GR_TSTP_3.4.1_C3
2. Test Details	To verify that the UDM sends deregistration notifications to NF consumers using the Nudm_UECM_DeregistrationNotification service as per 3GPP specifications.
3. Test Instruments Required	Wireshark, UE + gNB simulator tool
4. Test Setup	Test Setup Small size 5G Core-1
5. Test Procedure	Action • Establish NG setup between AMF and gNB. • Register the UE with 5G core • UE Initiates UE deregistration Request. Response: • UE deregistration procedures initiated and the UDM sent Nudm_UECM_DeregistrationNotification to AMF.
6. Test Limits	NA
7. Expected Results	UDM providing UECM deregistration notification to AMF

1.Test No	GR_TSTP_3.4.1_C4
2. Test Details	To verify that the UDM performs data retrieval operations based on different query parameters (PLMN, NSSAI, DNN) and maintains the subscriber session accordingly as per 3GPP specifications.
3. Test Instruments Required	Wireshark, UE + gNB simulator tool
4. Test Setup	Test Setup Small size 5G Core-1
5. Test Procedure	Action • Establish NG setup between AMF and gNB. • Register the UE with 5G core • Establish the PDU session Response: • UE successfully registered in 5G network and PDU has been established.
6. Test Limits	NA
7. Expected Results	UDM should be able to retrieve the provision data from UDR

1.Test No	GR_TSTP_3.4.1_C5
2. Test Details	UE To verify that the UDM supports UE authentication by providing updated authentication-related subscriber data to the subscribed NF consumer as per 3GPP specifications.
3. Test Instruments Required	Wireshark, UE + gNB simulator tool
4. Test Setup	Test Setup Small size 5G Core-1
5. Test Procedure	Action • Establish NG setup between AMF and gNB. • Register the UE with 5G core Response:s • UDM has generate authentication vector and sent to AUSF for authentication of UE in 5G network
6. Test Limits	NA
7. Expected Results	UDM is providing AV vector

1.Test No	GR_TSTP_3.4.1_C6
2. Test Details	To verify that the UDM subscribes to the AMF and notifies it when subscription data changes, as per 3GPP specifications.
3. Test Instruments Required	Wireshark, UE + gNB simulator tool
4. Test Setup	Test Setup Small size 5G Core-1
5. Test Procedure	Action • Establish NG setup between AMF and gNB. • Register the UE with 5G core • Establish the PDU session s Response: • UDM sent subscription notification to AMF when the AM data modified or updated.
6. Test Limits	NA
7. Expected Results	UDM providing subscription notify to AMF when AM data change

1.Test No	GR_TSTP_3.4.1_C7_1
2. Test Details	To verify that the UDM processes network-initiated deregistration requests from the AMF using the Nudm_UECM_DeregistrationNotification operation as per 3GPP specifications.
3. Test Instruments Required	Wireshark, UE + gNB simulator tool
4. Test Setup	Test Setup Small size 5G Core-1
5. Test Procedure	Action • Establish NG setup between AMF and gNB. • Register the UE with 5G core • NW(UDM) initiates De-Registration procedure. Response: • UDM sent the de-registration notification to AMF
6. Test Limits	NA
7. Expected Results	AMF send Downlink Deregistration Request to UE/RAN

1.Test No	GR_TSTP_3.4.1_C7_2
2. Test Details	To verify that the UDM supports authentication-related features, including: 1. Generation of 3GPP AKA authentication credentials. 2. Selection of the 5G-AKA authentication method, ensuring the AMF returns the UE's result to the AUSF. 3. Implementation of different protection schemes. 4. Support for de-concealment of the privacy-protected subscription identifier (SUCI), as per 3GPP specifications.
3. Test Instruments Required	Wireshark, UE + gNB simulator tool
4. Test Setup	Test Setup Small size 5G Core-1
5. Test Procedure	Action • Establish NG setup between AMF and gNB. • Register the UE with 5G core • Authentication Process • AMF Communication with AUSF Response: • AMF is communicating and the authentication is successfully result back to the AUSF.
6. Test Limits	NA
7. Expected Results	UDM is providing AV vector and convert SUCI into SUPI

1.Test No	GR_TSTP_3.4.1_C8
2. Test Details	To verify that the NRF supports the following services as per 3GPP specifications: 1. Nnrf_NFDiscovery service for discovering available network functions. 2. NFRegister, NFUpdate, and NFDeregister services for NF registration management. 3. NF Heart-Beat service to monitor the availability of registered NFs. 4. Deletion of stale security context to ensure security integrity. 5. Use of NF discovery service on expiry of validity period to refresh network function information.
3. Test Instruments Required	Wireshark, UE + gNB simulator tool
4. Test Setup	Test Setup Small size 5G Core-1
5. Test Procedure	Action • Establish NG setup between AMF and gNB. • Register the UE with 5G core • Establish the PDU session Response: • UDM successfully registered with NRF and send NF discovery request to NRF.
6. Test Limits	NA
7. Expected Results	UDM getting discovery, registration and subscription with NRF

1.Test No	GR_TSTP_3.4.1_D1
2. Test Details	Services (Get/Subscribe/ Unsubscribe/ Update) via the Nudm interface for subscriber data Management.
3. Test Instruments Required	Wireshark, UE + gNB simulator tool
4. Test Setup	UE + gNB simulator tool, AMF, SMF, UPF, UDM, AUSF, UDR, NRF, PCF, NEF, NSSF, BSF
5. Test Procedure	Action • Establish NG setup between AMF and gNB. • Register the UE with 5G core • Establish the PDU session Response: • The Nudm interface acknowledges the subscription request and starts successfully sending updates to the NF whenever the Get/Subscribe/ Unsubscribe/ Update changes.
6. Test Limits	NA
7. Expected Results	UDM is providing SDM data.

1.Test No	GR_TSTP_3.4.1_D2
2. Test Details	Verify UDM may support the EAP-based authentication method;
3. Test Instruments Required	Wireshark, UE + gNB simulator tool
4. Test Setup	UE + gNB simulator tool, AMF, SMF, UPF, UDM, AUSF, UDR, NRF, PCF, NEF, NSSF, BSF
5. Test Procedure	**Action:** • Establish NG setup between AMF and gNB. • UE initiates registration with 5G Core. • AMF forwards authentication request to AUSF. • AUSF requests authentication vectors from UDM using **EAP method**. • UDM provides EAP credentials or vectors to AUSF. • UE completes EAP authentication challenge. • Capture N8 and N12/N13 signaling using Wireshark. **Response:** • UDM correctly provides EAP credentials/vectors to AUSF. • AUSF successfully authenticates UE using EAP method. • Registration completes after successful EAP authentication.
6. Test Limits	NA
7. Expected Results	• UDM supports **EAP-based authentication** for 5G subscribers. • UE authentication using EAP-AKA’ or other EAP methods succeeds. • Correct signaling observed between **UDM ↔ AUSF ↔ AMF ↔ UE**. • Wireshark traces confirm EAP messages and proper authentication flow.

1.Test No	GR_TSTP_3.4.1_D3
2. Test Details	Verify that UDM data replication across multiple small size 5G Core network, which will enable UE to move from one small sized 5G Core network to another;
3. Test Instruments Required	Wireshark, UE + gNB simulator tool
4. Test Setup	UE + gNB simulator tool, AMF, SMF, UPF, UDM, AUSF, UDR, NRF, PCF, NEF, NSSF, BSF
5. Test Procedure	**Action:** • Register UE in 5GC-1 with active PDU session(s). • Replicate UE subscription and context data to UDM instance in 5GC-2. • UE moves (handover/registration) from 5GC-1 to 5GC-2. • AMF in 5GC-2 queries local UDM (replicated data) for UE context. • Capture signaling and context replication via Wireshark. **Response:** • UDM in 5GC-2 successfully receives replicated subscription and session data. • UE registration completes in 5GC-2 without re-authentication delay. • PDU session continuity maintained. • Correct signaling observed between AMF ↔ UDM ↔ UDR.
6. Test Limits	NA
7. Expected Results	• UDM supports **data replication** across multiple small-sized 5G Core networks. • UE can move between cores seamlessly, maintaining session and subscription data. • Registration and handover occur without loss of service or authentication failure. • Wireshark traces confirm correct **UDM ↔ AMF ↔ UDR** interactions and replicated data availability.

1.Test No	GR_TSTP_3.4.1_D4
2. Test Details	Below mentioned high level features: 5. Network slice selection; 6. Identification and authentication; 7. Access control and barring; and 8. Lawful Interception..
3. Test Instruments Required	Wireshark, UE + gNB simulator tool
4. Test Setup	UE + gNB simulator tool, AMF, SMF, UPF, UDM, AUSF, UDR, NRF, PCF, NEF, NSSF, BSF
5. Test Procedure	• Action • Establish NG setup between AMF and gNB. • Register the UE with 5G core • Establish the PDU session Response: • UE successfully authenticated and registered in 5G network with slice.
6. Test Limits	NA
7. Expected Results	UDM getting authentication and subscribe slice from UDR based on UE data provision

1.Test No	GR_TSTP_3.4.1_D5
2. Test Details	Generation and storage of keys using HSM to protect long-term keys from physical attacks and to keep them in the secure environment.
3. Test Instruments Required	Wireshark, UE + gNB simulator tool
4. Test Setup	UE + gNB simulator tool, AMF, SMF, UPF, UDM, AUSF, UDR, NRF, PCF, NEF, NSSF, BSF
5. Test Procedure	Action • In a 5G network, various cryptographic keys are used for authentication, integrity protection, and confidentiality. These keys are essential to secure communications and data exchanges within the network. Key generation involves creating these cryptographic keys based on wellestablished algorithms. Response: • UDM generates and store various cryptographic keys in a secure and random manner using HSM.
6. Test Limits	NA
7. Expected Results	UDM should generates and store various cryptographic keys in a secure and random manner using HSM to protect long-term keys from physical attacks and to keep them in the secure environment.

1.Test No	GR_TSTP_3.4.1_D6
2. Test Details	Interworking with HSS I) UDM shall provide support to Service based interfaces for direct UDM-HSS interworking; II) Terminating-Access Domain Selection for 5G access via UDM-HSS interworking; and III) P-CSCF restoration via UDM-HSS interworking.
3. Test Instruments Required	Wireshark, UE + gNB simulator tool
4. Test Setup	UE + gNB simulator tool, AMF, SMF, UPF, UDM, AUSF, UDR, NRF, PCF, NEF, NSSF, BSF
5. Test Procedure	Action • Establish NG setup between AMF and gNB. • Register the UE with 5G core • Establish the PDU session • 5G to 4G handover with N26 handover Response: • UDM's role in a successfully 5G to 4G handover is to manage userrelated data and ensure a seamless transition of services and context as the user moves from the 5G network to the 4G network.
6. Test Limits	NA
7. Expected Results	UDM is using in 5G to 4G handover

1.Test No	GR_TSTP_3.4.1_D7
2. Test Details	Following high level features: I) Network slice selection; II) Access control and barring; and III) Lawful Interception
3. Test Instruments Required	Wireshark, UE + gNB simulator tool
4. Test Setup	UE + gNB simulator tool, AMF, SMF, UPF, UDM, AUSF, UDR, NRF, PCF, NEF, NSSF, BSF
5. Test Procedure	Action • Establish NG setup between AMF and gNB. • Register the UE with 5G core • Authentication Process • AMF Communication with AUSF Response: • AMF is communicating and the authentication is successfully result back to the AUSF.
6. Test Limits	NA
7. Expected Results	UDM is providing AV vector and convert SUCI into SUPI

1.Test No	GR_TSTP_3.4.1_D8
2. Test Details	NFStatusSubscribe, I)NFStatusNotify, NFStatusUnSubscribe service; II) NFListRetrieval service; III) NFProfileRetrieval service; IV) Nnrf_AccessToken service; and V) Validation of expire time present in token validation response from NRF.
3. Test Instruments Required	Wireshark, UE + gNB simulator tool
4. Test Setup	UE + gNB simulator tool, AMF, SMF, UPF, UDM, AUSF, UDR, NRF, PCF, NEF, NSSF, BSF
5. Test Procedure	Action • Establish NG setup between AMF and gNB. • Register the UE with 5G core • Establish the PDU session Response: • UDM successfully registered with NRF and send NF discovery request to NRF.
6. Test Limits	NA
7. Expected Results	UDM getting discovery, registration and subscription with NRF

1.Test No	GR_TSTP_3.5.1_A
2. Test Details	To verify that the AUSF successfully connects with the UDM over N13 and the AMF over N12 using standard 3GPP interfaces.
3. Test Instruments Required	Wireshark, UE + gNB simulator tool
4. Test Setup	Test Setup Small size 5G Core-1
5. Test Procedure	Action • Establish NG setup between AMF and gNB. • Register the UE with 5G core • During the Authentication procedure, AUSF will communicate with the AMF and UDM. Response: • AUSF has been communicated with the UDM and AMF during the authentication procedure of UE.
6. Test Limits	NA
7. Expected Results	AUSF should communicate with the UDM and AMF during the authentication procedure of UE

1.Test No	GR_TSTP_3.5.1_B1
2. Test Details	To verify that the AUSF supports at least one authentication profile from Null, Profile-A, or Profile-B as per 3GPP specifications.
3. Test Instruments Required	Wireshark, UE + gNB simulator tool
4. Test Setup	Test Setup Small size 5G Core-1
5. Test Procedure	Action • Establish NG setup between AMF and gNB. • Send a UE registration request. • Null authentication is a scheme where no authentication is performed. It might be used in scenarios where authentication is not required or when specific security mechanisms are applied at higher layers. • Profile-A authentication involves the use of authentication vectors to validate the identity of the user equipment (UE). • Profile-B authentication is an advanced authentication scheme that enhances security by introducing additional factors, such as user-specific keys or additional authentication protocols. Response: • AUSF can support Different authentication schemes i.e., Null, Profile-A & Profile-B.
6. Test Limits	NA
7. Expected Results	AUSF should support Different authentication schemes i.e., Null, Profile-A & Profile-B.

1.Test No	GR_TSTP_3.5.1_B2
2. Test Details	To verify that the AUSF provides UE authentication services to the requesting NF using the Nausf_UEAuthentication service as per 3GPP specifications.
3. Test Instruments Required	Wireshark, UE + gNB simulator tool
4. Test Setup	Test Setup Small size 5G Core-1
5. Test Procedure	Action • Establish NG setup between AMF and gNB. • Register the UE with 5G core Response: • AUSF will provide the authentication service to the UE using Nausf_UEAuthentication request by the NF.
6. Test Limits	NA
7. Expected Results	AUSF should provide the authentication service to the UE using Nausf_UEAuthentication request by the NF.

1.Test No	GR_TSTP_3.5.1_B3
2. Test Details	To verify that the AUSF sets the authResult to AUTHENTICATION FAILURE if the UE fails authentication, as per 3GPP specifications.
3. Test Instruments Required	Wireshark, UE + gNB simulator tool
4. Test Setup	Test Setup Small size 5G Core-1
5. Test Procedure	Action • Establish NG setup between AMF and gNB. • Configure UE+RAN Simulator for Authentication failure • Register the UE with 5G core Response: • At the time of UE authentication procedure, AUSF will set authResult to AUTHENTICATION FAILURE if AUSF got invalid AUTN in the Authentication request message.
6. Test Limits	NA
7. Expected Results	At the time of UE authentication procedure,AUSF should set authResult to AUTHENTICATION FAILURE if AUSF got invalid AUTN in the Authentication request message.

1.Test No	GR_TSTP_3.5.1_B4
2. Test Details	To verify that the AUSF correctly supports and processes 5G-AKA procedures for UE authentication as per 3GPP specifications.
3. Test Instruments Required	Wireshark, UE + gNB simulator tool
4. Test Setup	Test Setup Small size 5G Core-1
5. Test Procedure	Action • Establish NG setup between AMF and gNB. • Register the UE with 5G core Response: • During the UE authentication procedure, AUSF will follow the 5G-AKA procedure.
6. Test Limits	NA
7. Expected Results	During the UE authentication procedure, AUSF should follow the 5G-AKA procedure.

1.Test No	GR_TSTP_3.5.1_B5
2. Test Details	To verify that the AUSF processes UE identity (e.g., SUPI or SUCI) and Serving Network Name in the "authenticate" service request received from an NF, as per 3GPP specifications.
3. Test Instruments Required	Wireshark, UE + gNB simulator tool
4. Test Setup	Test Setup Small size 5G Core-1
5. Test Procedure	Action • Establish NG setup between AMF and gNB. • Send a UE registration request to the network. • when a Network Function (NF) sends an "authenticate" service request to the Authentication Server Function (AuSF), two of the important parameters included in the "authenticate" service request are the UE identity (e.g., SUPI or SUCI) and the Serving Network Name. Let's explore these parameters. • The NF enables the AuSF to perform a secure and accurate authentication of the UE, ensuring that the correct subscriber is being authenticated within the proper network context. Response: • AUSF has been performed the authentication and ensured the correct subscriber is being authenticated within the proper network context
6. Test Limits	NA
7. Expected Results	AUSF should perform the authentication and ensure the correct subscriber is being authenticated within the proper network context.

1.Test No	GR_TSTP_3.5.1_B6
2. Test Details	To verify that the AUSF provides appropriate 4xx/5xx HTTP status codes with a Problem Details structure containing the "cause" attribute set to an application error upon failure in the 5G-AKA and/or 5G-EAP-AKA' procedure (if supported), as per 3GPP specifications.
3. Test Instruments Required	Wireshark, UE + gNB simulator tool
4. Test Setup	Test Setup Small size 5G Core-1
5. Test Procedure	Action • Establish NG setup between AMF and gNB. • Configure Core Network such that UE Authentication fails • Register the UE with 5G core Response: • AUSF will give the 4xx/5xx http error status codes if the Authentication procedure got fails
6. Test Limits	NA
7. Expected Results	AUSF should give the 4xx/5xx http error status codes if the Authentication procedure got fails.

1.Test No	GR_TSTP_3.5.1_B7
2. Test Details	To verify that the NRF supports the following services as per 3GPP specifications: 1. Nnrf_NFDiscovery service for discovering available network functions. 2. NFRegister, NFUpdate, and NFDeregister services for NF registration and lifecycle management. 3. NF Heart-Beat service to monitor the availability and status of registered NFs. 1. NFStatusSubscribe and NFStatusNotify services to enable NF consumers to subscribe to and receive notifications about NF status changes.
3. Test Instruments Required	Wireshark, UE + gNB simulator tool
4. Test Setup	Test Setup Small size 5G Core-1
5. Test Procedure	Action • The AUSF can utilize the Nnrf_NFDiscovery service to discover other network functions.The AUSF can register its availability and capabilities with the NRF using the NFRegister service. • The AUSF can update its registration information with the NRF using the NFUpdate service. When the AUSF needs to unregister or become unavailable, it can use the NFDeregister service to inform the network about its status change. • The NF Heart-Beat service involves periodic communication between the AUSF and the NRF to indicate the AUSF's active status and availability. Response: • AUSF has interacts with the NRF through various services to manage its registration, status, and discoverability within the 5G network.
6. Test Limits	NA
7. Expected Results	AUSF should interacts with the NRF through various services to manage its registration, status, and discoverability within the 5G network.

1.Test No	GR_TSTP_3.5.1_C1
2. Test Details	AuSF may support 5G- EAP- AKA' procedures.
3. Test Instruments Required	Wireshark, UE + gNB simulator tool
4. Test Setup	UE + gNB simulator tool, AMF, SMF, UPF, UDM, AUSF, UDR, NRF, PCF, NEF, NSSF, BSF
5. Test Procedure	Action • Establish NG setup between AMF and gNB. • Register the UE with 5G core Response: • During the UE authentication procedure, AUSF will follow the 5G-EAPAKA procedure
6. Test Limits	NA
7. Expected Results	During the UE authentication procedure, AUSF should follow the 5G-EAP-AKA procedure.

1.Test No	GR_TSTP_3.5.1_C2
2. Test Details	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. Test Instruments Required	Wireshark, UE + gNB simulator tool
4. Test Setup	UE + gNB simulator tool, AMF, SMF, UPF, UDM, AUSF, UDR, NRF, PCF, NEF, NSSF, BSF
5. Test Procedure	Action • When the previous access token issued by the NRF is about to expire or has already expired, the AUSF needs to request a new access token to continue its authorized interactions with the NRF. • The AUSF uses the NF Discovery service provided by the NRF to locate the appropriate service endpoint to send its access token request. • The AUSF sends an access token request to the designated service endpoint identified through the NF Discovery service.This request includes information about the AUSF's identity and its intention to obtain a new access token. • The NRF receives the access token request from the AUSF and processes it.The NRF validates the AUSF's identity and checks if the request for a new access token is valid. Response: • The AUSF ensured that it maintains continuous and authorized access to the NRF's services by obtaining and using valid access tokens.
6. Test Limits	NA
7. Expected Results	The AUSF should ensure that it maintains continuous and authorized access to the NRF's services by obtaining and using valid access tokens.

1.Test No	GR_TSTP_3.5.1_C3
2. Test Details	Both On-demand as well as Periodic/Scheduled backup procedures;
3. Test Instruments Required	Wireshark, UE + gNB simulator tool
4. Test Setup	UE + gNB simulator tool, AMF, SMF, UPF, UDM, AUSF, UDR, NRF, PCF, NEF, NSSF, BSF
5. Test Procedure	Action • AUSF would likely implement both on-demand and periodic/scheduled backup procedures to safeguard its data. • AUSF administrators can initiate on-demand backups manually when needed, such as before performing significant updates, changes, or maintenance procedures. • Periodic backups are carried out as background processes, ensuring minimal disruption to the AUSF's normal operations. Response: • By implementing both on-demand and periodic/scheduled backup procedures, the AUSF can effectively protect its data, ensure service continuity, and facilitate recovery in the event of data loss or system disruptions.
6. Test Limits	NA
7. Expected Results	By implementing both on-demand and periodic/scheduled backup procedures, the AUSF should effectively protect its data, ensure service continuity, and facilitate recovery in the event of data loss or system disruptions.

1.Test No	GR_TSTP_3.6.1_A
2. Test Details	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. Test Instruments Required	Wireshark, UE + gNB simulator tool
4. Test Setup	UE + gNB simulator tool, AMF, SMF, UPF, UDM, AUSF, UDR, NRF, PCF, NEF, NSSF, BSF
5. Test Procedure	Action • Establish NG setup between AMF and gNB. • Register the UE with 5G core • PDU session establishment • UDM will communicate with the UDR to retrieve user profile data and authentication information. • The PCF interacts with the UDR to retrieve policy-related information about a user's subscription and QoS (Quality of Service) requirements. • The NEF interacts with the UDR to expose network data to authorized third-party applications and services. Response: • UDR will provide the user profile data and authentication information to the UDM. UDR will provide policy-related information to PCF and UDR provides relevant user context data to the NEF.
6. Test Limits	NA
7. Expected Results	UDR should provide the user profile data and authentication information to the UDM and it should provide policy-related information to PCF and UDR provides relevant user context data to the NEF.

1.Test No	GR_TSTP_3.6.1_B1
2. Test Details	Authorization of user equipment.
3. Test Instruments Required	Wireshark, UE + gNB simulator tool
4. Test Setup	UE + gNB simulator tool, AMF, SMF, UPF, UDM, AUSF, UDR, NRF, PCF, NEF, NSSF, BSF
5. Test Procedure	Action • When a UE initiates a session or accesses network services, the network elements (such as the Access Network, PCF, AMF, etc.) involved in the process communicate with the UDR to retrieve the UE's subscription profile. • This subscription data is analyzed to determine what services or resources the UE is authorized to access. • The UDR's authorization process aligns with network policies defined by the operator. These policies specify which services or resources are allowed or restricted for specific subscription profiles. • Based on the analysis of the subscription data and policies, the UDR makes access control decisions. Response: • Based on the analysis, UDR determined that the UE is authorized to access the requested services.
6. Test Limits	NA
7. Expected Results	Based on the analysis, UDR should determine that the UE is authorized to access the requested services.

1.Test No	GR_TSTP_3.6.1_B2
2. Test Details	Storage of access and mobility data and session management data needed by NF consumers to implement application logic.
3. Test Instruments Required	Wireshark, UE + gNB simulator tool
4. Test Setup	UE + gNB simulator tool, AMF, SMF, UPF, UDM, AUSF, UDR, NRF, PCF, NEF, NSSF, BSF
5. Test Procedure	Action • AMF and SMF sends the request to UDR to store the access and mobility data and session management data. Response: • UDR has been stored the access and mobility data and session management data after it receives the request to store.
6. Test Limits	NA
7. Expected Results	UDR should be able to store the access and mobility data and session management data when it receives the request to store.

1.Test No	GR_TSTP_3.6.1_B3
2. Test Details	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.
3. Test Instruments Required	Wireshark, UE + gNB simulator tool
4. Test Setup	UE + gNB simulator tool, AMF, SMF, UPF, UDM, AUSF, UDR, NRF, PCF, NEF, NSSF, BSF
5. Test Procedure	Action • NF Consumer sends a request to UDR for the deletion of service profile for an existing user or profile for which consumer propose to remove an application data record when NF wants to deactivate their account. Response: • UDR has been deleted the service profile as per the NF consumer request.
6. Test Limits	NA
7. Expected Results	UDR should delete the service profile as per the NF consumer request.

1.Test No	GR_TSTP_3.6.1_B4
2. Test Details	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.
3. Test Instruments Required	Wireshark, UE + gNB simulator tool
4. Test Setup	UE + gNB simulator tool, AMF, SMF, UPF, UDM, AUSF, UDR, NRF, PCF, NEF, NSSF, BSF
5. Test Procedure	Action • NF Consumer sends a request to UDR for the creation of service profile for an existing user or NF service consumer intends to insert a new application data record into the UDR. Response: • UDR has been created the service profile as per the NF consumer request.
6. Test Limits	NA
7. Expected Results	UDR should create the service profile as per the NF consumer request.

1.Test No	GR_TSTP_3.6.1_B5
2. Test Details	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.
3. Test Instruments Required	Wireshark, UE + gNB simulator tool
4. Test Setup	UE + gNB simulator tool, AMF, SMF, UPF, UDM, AUSF, UDR, NRF, PCF, NEF, NSSF, BSF
5. Test Procedure	Action • Before any data access is allowed, the UDR ensures that the user or system attempting to access the data is authenticated and has the necessary credentials. • The UDR enforces authorization policies that define what types of data and services a user or system is allowed to access based on their role, subscription, and other attributes. • The UDR implements RBAC, where access permissions are assigned based on user roles. Users are granted access only to the data that is relevant to their roles. • ABAC allows access decisions based on various attributes such as user identity, time of access, location, and other contextual information. • The UDR ensures that users can access service data only at their authorized levels. For instance, subscribers may be allowed to access their own data but not data of other users. Response: • UDR can ensure that Authorization management mechanism to guarantee the safety of data access also access control.
6. Test Limits	NA
7. Expected Results	UDR should ensure that Authorization management mechanism to guarantee the safety of data access also access control.

1.Test No	GR_TSTP_3.6.1_B6_1
2. Test Details	User confidentiality protection functionalities: (I) Providing globally unique 5G Subscription Permanent Identifier (SUPI) to each subscriber in the 5G System and provisioned in the UDM/UDR; (II) Supporting Permanent Equipment Identifier (PEI) to assume different formats for different UE types and use cases;
3. Test Instruments Required	Wireshark, UE + gNB simulator tool
4. Test Setup	UE + gNB simulator tool, AMF, SMF, UPF, UDM, AUSF, UDR, NRF, PCF, NEF, NSSF, BSF
5. Test Procedure	Action • Establish NG setup between AMF and gNB. • Register the UE with 5G core • PDU session establishment • UDR will provides the globally unique 5G Subscription Permanent Identifier (SUPI) to each subscriber in the 5G System When a new subscriber registers with the 5G network. Response: • The UDM has initiated the process of assigning a SUPI to the subscriber. UDR generates a unique SUPI for the subscriber.
6. Test Limits	NA
7. Expected Results	UDR should provide the globally unique 5G Subscription Permanent Identifier (SUPI) to each subscriber.

1.Test No	GR_TSTP_3.6.1_B6_2
2. Test Details	User confidentiality protection functionalities: (III) And HTTP GET and HTTP POST method for Query and subscribe operation; and (IV) Ability to identify and remove inconsistent data.
3. Test Instruments Required	Wireshark, UE + gNB simulator tool
4. Test Setup	UE + gNB simulator tool, AMF, SMF, UPF, UDM, AUSF, UDR, NRF, PCF, NEF, NSSF, BSF
5. Test Procedure	**Action:** • Establish secure SBI communication between NFs using HTTPS/TLS. • From a registered NF, perform **HTTP GET** for query and **HTTP POST** for subscription to another NF (e.g., UDM → UDR). • Observe confidentiality protection (TLS encryption, authorized access tokens, no clear-text user data). • Introduce inconsistent or duplicate user data entries in UDR. • Trigger NF synchronization or consistency check function. • Observe the NF response for identification and removal of inconsistent data entries. **Response:** • HTTP messages are transmitted securely using TLS. • Authorization tokens validated successfully. • UDR identifies and removes or corrects inconsistent records.
6. Test Limits	NA
7. Expected Results	• All **HTTP GET/POST operations** for Query and Subscribe are executed over **TLS-secured channels** ensuring **user confidentiality**. • Only **authorized NFs** can perform operations — verified by access tokens in headers. • **No user data exposed in clear text** during transmission or logging. • **Inconsistent or duplicate data** in UDR/UDM database are successfully identified and removed or corrected automatically or via triggered cleanup. • Logs and packet captures confirm successful confidentiality protection and data integrity restoration.

1.Test No	GR_TSTP_3.6.1_C1
2. Test Details	Nudr_DataRepository services:-Service operations like Create, Delete, Update, Notify, Subscribe, unsubscribe;
3. Test Instruments Required	Wireshark, UE + gNB simulator tool
4. Test Setup	UE + gNB simulator tool, AMF, SMF, UPF, UDM, AUSF, UDR, NRF, PCF, NEF, NSSF, BSF
5. Test Procedure	Action • NF consumers sends service operations requests like Create, Delete, Update, Notify, Subscribe, unsubscribe to UDR. Response: • UDR has performed the service operations like Creation, Deletion, Update, Notifying, Subscribing, unsubscribing and sends responses to the NF consumers.
6. Test Limits	NA
7. Expected Results	UDR should perform all the service operations and it should send responses to the consumers.

1.Test No	GR_TSTP_3.6.1_C2
2. Test Details	User confidentiality protection functionalities: I) Monitoring of various events configured via UDM
3. Test Instruments Required	Wireshark, UE + gNB simulator tool
4. Test Setup	UE + gNB simulator tool, AMF, SMF, UPF, UDM, AUSF, UDR, NRF, PCF, NEF, NSSF, BSF
5. Test Procedure	Action • Establish NG setup between AMF and gNB. • Register the UE with 5G core • PDU session establishment • UDR will provides the globally unique 5G Subscription Permanent Identifier (SUPI) to each subscriber in the 5G System When a new subscriber registers with the 5G network. Response: • The UDM has initiated the process of assigning a SUPI to the subscriber. UDR generates a unique SUPI for the subscriber.
6. Test Limits	NA
7. Expected Results	UDR should provide the globally unique 5G Subscription Permanent Identifier (SUPI) to each subscriber.

1.Test No	GR_TSTP_3.6.1_C3
2. Test Details	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
3. Test Instruments Required	Wireshark, UE + gNB simulator tool
4. Test Setup	UE + gNB simulator tool, AMF, SMF, UPF, UDM, AUSF, UDR, NRF, PCF, NEF, NSSF, BSF
5. Test Procedure	Action • Load balancing distributes incoming traffic and requests across multiple UDR instances to ensure even distribution of processing loads. The UDR can implement load balancing algorithms that consider factors such as server capacity, current load, and network latency. • n an active-active redundancy model, multiple UDR instances are actively processing traffic simultaneously. Load balancing evenly distributes traffic across all active instances, ensuring optimal resource utilization. • n an active-passive redundancy model, one UDR instance (the active node) processes traffic, while the others (passive nodes) stand by in case of a failure. If the active node fails, traffic is automatically redirected to a passive node. • The UDR continuously monitors its resource utilization, including CPU usage, memory usage, and network traffic. An overload threshold value is predefined based on the UDR's capacity and performance characteristics. • The UDR adjusts its resource allocation dynamically based on the incoming load and the predefined threshold value. Once the monitored resource utilization crosses the threshold value, the UDR identifies that an overload condition is approaching. • The UDR triggers an alarm system to notify administrators or network management systems about the impending overload. Response: • UDR can perform the load balancing functionalities according to the situation.

6. Test Limits	NA
7. Expected Results	UDR should perform the load balancing functionalities according to the situation.

1.Test No	GR_TSTP_3.6.1_C4
2. Test Details	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.
3. Test Instruments Required	Wireshark, UE + gNB simulator tool
4. Test Setup	UE + gNB simulator tool, AMF, SMF, UPF, UDM, AUSF, UDR, NRF, PCF, NEF, NSSF, BSF
5. Test Procedure	Action • Data redundancy involves maintaining duplicate copies of data to ensure availability in case of hardware failures or data corruption. Site-level redundancy focuses on duplicating UDR instances across geographically separated sites to enhance resilience against site-specific failures. Network redundancy ensures that communication paths remain available even if there's a network failure. • By performing Redundancy and Load balancing, Geographical redundancy, Active-Passive failover mechanisms, UDR can ensure high availability. • Geographical redundancy involves deploying UDR instances in multiple geographically separated data centers. Response: • UDR has enforced different redundancy mechanism procedures according to the situation.
6. Test Limits	NA
7. Expected Results	UDR should enforce different redundancy mechanism procedures according to the situation.

1.Test No	GR_TSTP_3.6.1_C5
2. Test Details	Verify 1+1 or 1+1+1 redundancy at data service level.
3. Test Instruments Required	Wireshark, UE + gNB simulator tool
4. Test Setup	UE + gNB simulator tool, AMF, SMF, UPF, UDM, AUSF, UDR, NRF, PCF, NEF, NSSF, BSF
5. Test Procedure	**Action:** • Establish NG setup between AMF and gNB. • Register UE and initiate PDU session(s). • SMF/UDM queries subscription/policy data from primary UDR. • Simulate failure of primary UDR instance. • Verify that queries are automatically redirected to redundant UDR instance. • Capture signaling over Nudr interface using Wireshark. **Response:** • UDR redundancy ensures continued access to subscription and policy data. • SMF/UDM queries succeed without service interruption. • Signaling correctly switches to redundant instance upon primary failure.
6. Test Limits	NA
7. Expected Results	• 1+1 or 1+1+1 redundancy operates correctly for UDR data services. • Subscription and policy data are continuously accessible even during UDR failure. • SMF/UDM successfully retrieves required data from redundant UDR instance. • Wireshark traces confirm redundancy signaling and uninterrupted data access.

1.Test No	GR_TSTP_3.6.1_C6
2. Test Details	Following NRF services:5 (Optional) (I) NFStatusSubscribe, NFStatusUnsubscribe, NFRegister; (II) NFUpdate, NFDeregister, NFListRetrieval, NFProfileRetrieval; (III) Nnrf_AccessToken service, Heat Beat Service mechanism; (IV) Nnrf_NFManagement service; and (V) Nnrf_NFDiscovery service.
3. Test Instruments Required	Wireshark, UE + gNB simulator tool
4. Test Setup	UE + gNB simulator tool, AMF, SMF, UPF, UDM, AUSF, UDR, NRF, PCF, NEF, NSSF, BSF
5. Test Procedure	Action • Establish NG setup between AMF and gNB. • Register the UE with 5G core • Establish the PDU session Response: • UDM successfully registered with NRF and send NF discovery request to NRF.
6. Test Limits	NA
7. Expected Results	UDM getting discovery, registration and subscription with NRF.

1.Test No	GR_TSTP_3.7.1_A
2. Test Details	To verify that NRF shall be connected with other 3GPP network elements using standard Service Based Interface (SBI) III) AMF; IX) SMF (X) UDM; XI) AUSF; XII) NEF; III) PCF; and IV) NSSF.
3. Test Instruments Required	Wireshark, UE + gNB simulator tool
4. Test Setup	Test Setup Small size 5G Core-1
5. Test Procedure	Action • All 5G core nodes running properly. • All nodes will get registered with NRF. Response: NRF has stored all the registered nodes data.
6. Test Limits	NA
7. Expected Results	NRF should store all the registered nodes data.

1.Test No	GR_TSTP_3.7.1_B
2. Test Details	To verify that NRF may be connected with other 3GPP network elements using standard Service Based Interface (SBI) (I) SMSF; (II) UPF.
3. Test Instruments Required	Wireshark, UE + gNB simulator tool
4. Test Setup	Test Setup Small size 5G Core-1
5. Test Procedure	Action • All 5G core nodes running properly. • All nodes will get registered with NRF. Response: NRF has stored all the registered nodes data.
6. Test Limits	NA
7. Expected Results	NRF should store all the registered nodes data.

1.Test No	GR_TSTP_3.7.1_C1
2. Test Details	To verify that Following services: (X) Nnrf_NFManagement service; (XI) Nnrf_NFDiscovery service; XII) NFRegister service; (III) NFUpdate service; (IV) NF Heart-Beat service; XV) NFDeregister service; (VI) NFStatusSubscribe service; VII) NFStatusNotify service; (III) NFStatusUnSubscribe service;
3. Test Instruments Required	Wireshark, UE + gNB simulator tool
4. Test Setup	Test Setup Small size 5G Core-1
5. Test Procedure	Action • NFS send GET /nnrf-disc/v1/nf-instances?target-nf type=NFs1&requester-nf-type=NFs2to NRF Response: • NRF send 200 OK
6. Test Limits	NA
7. Expected Results	NRF should send 200 OK

1.Test No	GR_TSTP_3.7.1_C2
2. Test Details	To verify Subscription and notification to other NFs regarding the registration in NRF of new NF instances of a given type.
3. Test Instruments Required	Wireshark, UE + gNB simulator tool
4. Test Setup	Test Setup Small size 5G Core-1
5. Test Procedure	Action • Nfs send POST /nnrf-nfm/v1/subscriptions HTTP to NRF Response: • NRF send 201 OK
6. Test Limits	NA
7. Expected Results	NRF should send 201 OK

1.Test No	GR_TSTP_3.7.1_C3
2. Test Details	To verify that Subscription of NF to be notified of registration, deregistration and profile changes of NF Instances, along with their potential NF services
3. Test Instruments Required	Wireshark, UE + gNB simulator tool
4. Test Setup	Test Setup Small size 5G Core-1
5. Test Procedure	Action • Nfs send POST /pcf/nrf-notifications to NRF Response: • NRF send 204
6. Test Limits	NA
7. Expected Results	NRF should send 204

1.Test No	GR_TSTP_3.7.1_C4
2. Test Details	To verify that 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.
3. Test Instruments Required	Wireshark, UE + gNB simulator tool
4. Test Setup	Test Setup Small size 5G Core-1
5. Test Procedure	Action • Nf's send list retrival request for any NF to NRF Response: • NRF will send complete list of NF profile
6. Test Limits	NA
7. Expected Results	NRF should send complete list of NF profile

1.Test No	GR_TSTP_3.7.1_C5
2. Test Details	To verify that 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
3. Test Instruments Required	Wireshark, UE + gNB simulator tool
4. Test Setup	Test Setup Small size 5G Core-1
5. Test Procedure	Action • All 5G core nodes running properly. • All nodes will get registered with NRF. • All nodes connect with each other with their particular URL. Response: • NRF has stored all the registered nodes data
6. Test Limits	NA
7. Expected Results	NRF should store all the registered nodes data

1.Test No	GR_TSTP_3.7.1_C6
2. Test Details	Support for NFDeregister Service request.
3. Test Instruments Required	Wireshark, UE + gNB simulator tool
4. Test Setup	Test Setup Small size 5G Core-1
5. Test Procedure	**Action:** • Register NF instance (e.g., AMF, SMF) with NRF. • Initiate **NF Deregister service request** from the NF to NRF. • NRF processes the deregistration request. • Capture signaling between NF ↔ NRF using Wireshark. **Response:** • NRF removes the NF from its repository. • NRF returns confirmation response to NF. • Other NFs attempting to discover the deregistered NF do not receive it in discovery results.
6. Test Limits	NA
7. Expected Results	• NF Deregister service request is successfully supported. • NRF updates its repository and confirms deregistration. • NF is no longer discoverable in the NRF. • Wireshark traces confirm correct deregistration signaling as per **3GPP TS 29.510**.

1.Test No	GR_TSTP_3.7.1_D1
2. Test Details	To verify that Following services: (V) Nnrf_AccessToken service; (VI) Nnrf_Bootstrapping service (VII) NFListRetrieval service; and NFProfileRetrieval service
3. Test Instruments Required	Wireshark, UE + gNB simulator tool
4. Test Setup	Test Setup Small size 5G Core-1
5. Test Procedure	Action • Establish NG setup between AMF and gNB. • Register the UE with 5G core • Establish the PDU session . Response: • UDM successfully registered with NRF and send NF discovery request to NRF.
6. Test Limits	NA
7. Expected Results	UDM getting discovery, registration and subscription with NRF

1.Test No	GR_TSTP_3.7.1_D2
2. Test Details	Verify that Deployment on shared-slice level (the NRF is configured with information belonging to a set of Network Slices).
3. Test Instruments Required	Wireshark, UE + gNB simulator tool
4. Test Setup	Test Setup Small size 5G Core-1
5. Test Procedure	Action • Establish NG setup between AMF and gNB. • Register the UE with 5G core with the particular Slice. Response: • PDU session will be established with information belonging to a set of Network Slices..
6. Test Limits	NA
7. Expected Results	PDU session should established with information belonging to a set of Network Slices.

1.Test No	GR_TSTP_3.7.1_D3
2. Test Details	Verify that Data structures and URI query parameters as defined in 3GPP TS 29.510 Clause 6.1.3.2.3.1.
3. Test Instruments Required	Wireshark, UE + gNB simulator tool
4. Test Setup	Test Setup Small size 5G Core-1
5. Test Procedure	Action • "NFS send POST /nnrf-nfm/v1/subscriptions as per 3gpp specs with data {""nfStatusNotificationUri"": ""http://172.16.5.23:9000/udm/nrfnotifications"", ""subscrCond"": {""NfTypeCond"": {""nfType"": ""AUSF""}}" Response: • "NRF send 201 OK {""nfStatusNotificationUri"":""http://172.16.5.23:9000/udm/nrfnotifications"",""subscrCond"":{""NfTypeCond"":{""nfType"":""AUSF""}},""sub scriptionId"":""480171WBF20220627054358""}"
6. Test Limits	NA
7. Expected Results	NRF should send 201 OK

1.Test No	GR_TSTP_3.7.1_D4
2. Test Details	Verify that Ability to send requests to SEPP in weighted or priority mode or combination of these.
3. Test Instruments Required	Wireshark, UE + gNB simulator tool
4. Test Setup	Test Setup Small size 5G Core-1
5. Test Procedure	Action • In weighted mode, assign different weights or numerical values to different SEPPs based on factors like capacity, performance, or proximity. Higher weights indicate higher priority. • In priority mode, assign specific priority levels (such as high, medium, and low) to SEPPs based on predefined criteria. Requests to SEPPs with higher priority are processed first. Response: • By implementing weighted, priority, or a combination of both modes, we can optimize the utilization of SEPP resources and ensure that requests are processed with the appropriate level of importance and efficiency.
6. Test Limits	NA
7. Expected Results	By implementing weighted, priority, or a combination of both modes, we can optimize the utilization of SEPP resources and ensure that requests are processed with the appropriate level of importance and efficiency.

1.Test No	GR_TSTP_3.7.1_D5
2. Test Details	Verify that Blocking of Register operation to be invoked from an NRF in a different PLMN.
3. Test Instruments Required	Wireshark, UE + gNB simulator tool
4. Test Setup	Test Setup Small size 5G Core-1
5. Test Procedure	Action • When an NRF receives a Register operation request from an AUSF or another network element, it should validate the PLMN identity associated with the request • The NRF compares the PLMN identity of the incoming request with its own PLMN identity. If they match, the request is processed as usual. • If the PLMN identity of the incoming request doesn't match the PLMN identity of the NRF, the NRF should reject the Register operation request. Response: • NRF has supported the blocking of register operation
6. Test Limits	NA
7. Expected Results	NRF should supported the blocking of register operation

1.Test No	GR_TSTP_3.7.1_D6
2. Test Details	Verify that Configuration with multiple PLMN IDs and registering, updating and deregistering the profile of Network Function Instances from any of these PLMN IDs.
3. Test Instruments Required	Wireshark, UE + gNB simulator tool
4. Test Setup	Test Setup Small size 5G Core-1
5. Test Procedure	Action • NFS send PUT /nnrf-nfm/v1/nf-instances/Nfs-ID to NRF {""nfInstanceId"": ""f9208ceb-970d-4d3d-8e67-5f390c01e121"", ""nfType"": ""NSSAAF"", ""nfStatus"": ""REGISTERED"", ""fqdn"": ""http://nssaaf-service:80""} Response: • NRF send 201 OK
6. Test Limits	NA
7. Expected Results	NRF should send 201 OK

1.Test No	GR_TSTP_3.7.1_D7
2. Test Details	Verify that 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
3. Test Instruments Required	Wireshark, UE + gNB simulator tool
4. Test Setup	Test Setup Small size 5G Core-1
5. Test Procedure	Action • The NRF continuously monitors the operational status of registered NFs using the NF Heart-Beat procedure or other relevant monitoring mechanisms. • The NF Heart-Beat procedure involves regular exchanges of messages between the NRF and the NF to confirm that the NF is operational and responsive • When the NRF determines that an NF is non-operative, it changes the NF's status to "SUSPENDED." Response: • NRF will set the NFStatus of a NF to SUSPENDED if it determines that the NF is non-operative.
6. Test Limits	NA
7. Expected Results	NRF should set the NFStatus of a NF to SUSPENDED if it determines that the NF is non-operative

1.Test No	GR_TSTP_3.7.1_D8
2. Test Details	Verify that Forwarding subscription request on basis of (target) PLMN-ID & NF-type if preconfigured routing policy is present. Precedence shall be given to routing Policy
3. Test Instruments Required	Wireshark, UE + gNB simulator tool
4. Test Setup	UE + gNB simulator tool, AMF, SMF, UPF, UDM, AUSF, UDR, NRF, PCF, NEF, NSSF, BSF
5. Test Procedure	Action • Establish a set of pre-configured routing policies that define how subscription requests should be forwarded based on target PLMN-ID and NF-type. • When a subscription request is received, evaluate the request against the pre-configured routing policies and criteria. • If a matching routing policy exists for the target PLMN-ID and NF-type in the subscription request, follow the instructions specified in that policy. • If there is no matching routing policy, or if the routing policy does not cover the combination of PLMN-ID and NF-type, proceed with the default behavior. Response: • Based on the matching routing policy or default behavior, decide which NF(s) the subscription request should be forwarded to.
6. Test Limits	NA
7. Expected Results	Based on the matching routing policy or default behavior, decide which NF(s) the subscription request should be forwarded to.

1.Test No	GR_TSTP_3.7.1D9
2. Test Details	Verify that 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.
3. Test Instruments Required	Wireshark, UE + gNB simulator tool
4. Test Setup	Test Setup Small size 5G Core-1
5. Test Procedure	Action • NRF-2 establishes a direct communication link with the NF Service Consumer. Instead of involving NRF-1 as an intermediary for subscription notifications, NRF-2 communicates directly with the NF Service Consumer. • When a subscription-related event occurs that requires notification, NRF2 triggers the event and prepares the necessary information for the POST request.NRF-2 sends a POST request containing the subscription notification data directly to the NF Service Consumer • The NF Service Consumer receives the POST request, processes the subscription notification, and performs any required actions. Response: • NRF-2 has sent a POST request directly to the NF consumer.
6. Test Limits	NA
7. Expected Results	NRF-2 should send a POST request directly to the NF consumer.

1.Test No	GR_TSTP_3.7.1_D10
2. Test Details	Verify that 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.
3. Test Instruments Required	Wireshark, UE + gNB simulator tool
4. Test Setup	Test Setup Small size 5G Core-1
5. Test Procedure	Action • NFS send PATCH /nnrf-nfm/v1/nf-instances/8e62f03e-bc17-4444-a43d60a0d55a026a to NRF Response: "NRF send 200 Ok • {""validityPeriod"":0,""nfInstances"":[{""nfInstanceId"":""8e62f03e-bc17-4444-a43d60a0d55a026a"",""nfType"":""AUSF"",""nfStatus"":""REGISTERED"",""heartBeat Timer"":60,""fqdn"":""http://ausfservice:8000"",""nfServicePersistence"":false,""nfProfileChangesInd"":false}]}"
6. Test Limits	NA
7. Expected Results	NRF should send 200 Ok

1.Test No	GR_TSTP_3.7.1_D11
2. Test Details	Verify that 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.
3. Test Instruments Required	Wireshark, UE + gNB simulator tool
4. Test Setup	Test Setup Small size 5G Core-1
5. Test Procedure	Action • NFS send PATCH /nnrf-nfm/v1/nf-instances/8e62f03e-bc17-4444-a43d60a0d55a026a to NRF Response: "NRF send 200 Ok • {""validityPeriod"":0,""nfInstances"":[{""nfInstanceId"":""8e62f03e-bc17-4444-a43d60a0d55a026a"",""nfType"":""AUSF"",""nfStatus"":""REGISTERED"",""heartBeat Timer"":60,""fqdn"":""http://ausfservice:8000"",""nfServicePersistence"":false,""nfProfileChangesInd"":false}]}"
6. Test Limits	NA
7. Expected Results	NRF should send 200 Ok

1.Test No	GR_TSTP_3.7.1_D12
2. Test Details	Verify that 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.Section 5.3.2.2.2.
3. Test Instruments Required	Wireshark, UE + gNB simulator tool
4. Test Setup	Test Setup Small size 5G Core-1
5. Test Procedure	Action • Classify software and hardware faults based on their severity and potential impact on the system. Categorize faults into different levels of severity, such as critical, major, minor, and informational. • Define a range of recovery strategies that correspond to the severity levels of faults • Evaluate the potential impact of each fault severity level on system operation, performance, and user experience. Consider factors like service disruption, data loss, and user inconvenience Response: • Implement recovery mechanisms that are tailored to the different fault severity levels i.e., Critical Faults, Major Faults, Minor Faults and Informational Faults
6. Test Limits	NA
7. Expected Results	Recovery mechanisms should be implemented that are tailored to the different fault severity levels i.e., Critical Faults, Major Faults, Minor Faults and Informational Faults

1.Test No	GR_TSTP_3.7.1_D13
2. Test Details	Verify that Establishment of connection with Secondary SEPP IP for forwarding the same request, in case when request timeout is received from Primary SEPP IP..
3. Test Instruments Required	Wireshark, UE + gNB simulator tool
4. Test Setup	Test Setup Small size 5G Core-1
5. Test Procedure	Action • Configure both Primary and Secondary SEPP IP addresses in the relevant network elements, such as load balancers, routers, and Nfs. • Continuously monitor the health and availability of the Primary SEPP IP by sending periodic health check requests • If a request to the Primary SEPP IP times out or if a response indicating a failure is received, consider it a trigger for a potential issue. Upon detecting a timeout or failure, initiate an automatic failover mechanism that switches the traffic to the Secondary SEPP IP Response: • Implement recovery mechanisms that are tailored to the different fault severity levels i.e., Critical Faults, Major Faults, Minor Faults and Informational Faults
6. Test Limits	NA
7. Expected Results	Connection has established to the secondary SEPP IP to forward the same request that previously timed out on the primary SEPP IP.

1.Test No	GR_TSTP_3.7.1_D14
2. Test Details	Verify that Geo-redundancy and disaster recovery architecture without any data loss or service outage.
3. Test Instruments Required	Wireshark, UE + gNB simulator tool
4. Test Setup	Test Setup Small size 5G Core-1
5. Test Procedure	Action • Implement real-time or near-real-time data replication between primary and secondary data centers in different geographic locations. • Set up an active-active configuration where both primary and secondary sites are actively serving traffic. • Utilize intelligent load balancers to distribute traffic across active data centers while considering factors like latency, load, and proximity. • Implement global traffic management to direct users to the nearest active data center based on their geographical location. Response: • By meticulously implementing geo-redundancy and disaster recovery strategies, we can minimize service disruptions, data loss, and downtime, providing users with a seamless and reliable experience even in the face of unexpected events.
6. Test Limits	NA
7. Expected Results	By meticulously implementing geo-redundancy and disaster recovery strategies, we can minimize service disruptions, data loss, and downtime, providing users with a seamless and reliable experience even in the face of unexpected events.

1.Test No	GR_TSTP_3.7.1_D15
2. Test Details	Roaming - Communication with H-NRF to resolve the home PLMN network functions over N27 interface via SEPP.
3. Test Instruments Required	Wireshark, UE + gNB simulator tool
4. Test Setup	Test Setup Small size 5G Core-1
5. Test Procedure	**Action:** • UE registers in V-PLMN with active PDU session(s). • V-NRF queries H-NRF over **N27 interface via SEPP** to discover home network functions. • SEPP enforces security and routes requests between V-NRF and H-NRF. • Capture signaling on N27 and SEPP using Wireshark. **Response:** • H-NRF responds to V-NRF with requested network function information. • V-PLMN NFs can successfully discover and interact with H-PLMN NFs. • SEPP logs show secure routing of messages between PLMNs.
6. Test Limits	NA
7. Expected Results	• Communication over **N27 via SEPP** is successfully established. • V-NRF resolves H-NRF and home PLMN NFs correctly. • Discovery and inter-PLMN interactions succeed for roaming UE. • Wireshark traces confirm proper **N27 and SEPP signaling** as per **3GPP TS 29.510**.

1.Test No	GR_TSTP_3.8.1_A1
2. Test Details	The PCF shall support: Interactions with the access and mobility policy enforcement in the AMF, through service-based interfaces;
3. Test Instruments Required	Wireshark, UE + gNB simulator tool
4. Test Setup	UE + gNB simulator tool, AMF, SMF, UPF, UDM, AUSF, UDR, NRF, PCF, NEF, NSSF, BSF
5. Test Procedure	Action • Establish NG setup between AMF and gNB. • Register the UE with 5G core • Establish the PDU session • PCF interacts with the AMF through service-based interfaces for the purpose of policy enforcement. This interaction allows the PCF to communicate policy and QoS-related information to the AMF and vice versa. Response: • PCF has interacted with the AMF through service-based interfaces to communicate policy and QoS-related information to the AMF and vice versa.
6. Test Limits	NA
7. Expected Results	PCF should interact with the AMF through service-based interfaces to communicate policy and QoS-related information to the AMF and vice versa.

1.Test No	GR_TSTP_3.8.1_A2
2. Test Details	Decision taking based upon subscription information, Access Type and the RAT Type.
3. Test Instruments Required	Wireshark, UE + gNB simulator tool
4. Test Setup	UE + gNB simulator tool, AMF, SMF, UPF, UDM, AUSF, UDR, NRF, PCF, NEF, NSSF, BSF
5. Test Procedure	Action • Subscription information refers to the specific details of a user's subscription plan and service agreements. The PCF uses subscription information to determine the user's entitlements, such as the data plan limits, service packages, and QoS levels associated with their subscription. • Access type refers to how a user is connecting to the network. It could be via 5G, 4G LTE, Wi-Fi, or other access technologies. The PCF considers the access type to adjust policies and QoS settings to suit the characteristics of the specific access technology. • RAT type refers to the specific radio technology being used for communication, such as 5G NR (New Radio) or LTE. The PCF takes into account the RAT type to optimize resource allocation and QoS for that specific technology. Response: • The PCF's ensured that network resources are allocated efficiently, users receive the expected QoS, and network performance is optimized based on the user's subscription information, Access Type and the RAT Type.
6. Test Limits	NA
7. Expected Results	The PCF should enforce policies related to data usage, bandwidth allocation, and service prioritization.

1.Test No	GR_TSTP_3.8.1_A3
2. Test Details	Handling of UE Context Establishment request as a part of UE Registration;
3. Test Instruments Required	Wireshark, UE + gNB simulator tool
4. Test Setup	UE + gNB simulator tool, AMF, SMF, UPF, UDM, AUSF, UDR, NRF, PCF, NEF, NSSF, BSF
5. Test Procedure	Action • Establish NG setup between AMF and gNB. • Register the UE with 5G core • Establish a PDU session Response: • As part of the UE context establishment process, the PCF communicated the assigned QoS parameters and policies to other network functions, such as the Access and Mobility Management Function (AMF) and the User Plane Function (UPF). These functions will then ensure that the UE's data traffic is treated according to the assigned policies and QoS settings.
6. Test Limits	NA
7. Expected Results	PCF should apply the appropriate policies and QoS rules during the UE Context Establishment procedure as a part of UE Registration.

1.Test No	GR_TSTP_3.8.1_A4
2. Test Details	The capability to take a PCC rule into service, and out of service, at a specific time of day;
3. Test Instruments Required	Wireshark, UE + gNB simulator tool
4. Test Setup	UE + gNB simulator tool, AMF, SMF, UPF, UDM, AUSF, UDR, NRF, PCF, NEF, NSSF, BSF
5. Test Procedure	Action • At a specific time of day, the PCF can activate or "take into service" a specific PCC rule. This might involve enabling a rule that provides enhanced QoS during peak hours or allows for additional data usage during off-peak hours • Similarly, at a different time of day, the PCF can deactivate or "take out of service" a specific PCC rule. This could involve disabling a rule that provides specific privileges or limits during certain time periods. Response: • The PCF's managed policy rules based on time allows for dynamic adjustments to accommodate changing network conditions and user behaviors.
6. Test Limits	NA
7. Expected Results	The PCFs should be able to manage policy rules based on time allows for dynamic adjustments to accommodate changing network conditions and user behaviors.

1.Test No	GR_TSTP_3.8.1_A5
2. Test Details	Session management related functionality of PDU Session related policy control
3. Test Instruments Required	Wireshark, UE + gNB simulator tool
4. Test Setup	UE + gNB simulator tool, AMF, SMF, UPF, UDM, AUSF, UDR, NRF, PCF, NEF, NSSF, BSF
5. Test Procedure	Action • Establish NG setup between AMF and gNB. • Register the UE with 5G core • Establish a PDU session • The PCF is responsible for enforcing policy rules that define how network resources are allocated and how services are treated. Response: • PCF has been enforced the Session management related functionality of PDU Session related policy control.
6. Test Limits	NA
7. Expected Results	PCF should enforce the Session management related functionality of PDU Session related policy control.

1.Test No	GR_TSTP_3.8.1_A6
2. Test Details	The capability to indicate to the SMF that a PCC rule shall be bound to the specified QoS flow (including default QoS flow).
3. Test Instruments Required	Wireshark, UE + gNB simulator tool
4. Test Setup	UE + gNB simulator tool, AMF, SMF, UPF, UDM, AUSF, UDR, NRF, PCF, NEF, NSSF, BSF
5. Test Procedure	Action • Establish NG setup between AMF and gNB. • Register the UE with 5G core • Establish a PDU session • The PCF can indicate to the SMF that a particular PCC rule should be applied to a specific QoS flow within the PDU session. • The PCF can also indicate that a PCC rule should be applied to the default QoS flow, which represents traffic that doesn't match any specific QoS flow criteria. Response: • The PCF has communicated with the SMF to provide information about the PCC rules and their associations with QoS flows.
6. Test Limits	NA
7. Expected Results	The PCF should communicate with the SMF to provide information about the PCC rules and their associations with QoS flows.

1.Test No	GR_TSTP_3.8.1_A7
2. Test Details	Control of QoS for the packet traffic of the PDU Session.
3. Test Instruments Required	Wireshark, UE + gNB simulator tool
4. Test Setup	UE + gNB simulator tool, AMF, SMF, UPF, UDM, AUSF, UDR, NRF, PCF, NEF, NSSF, BSF
5. Test Procedure	Action • Establish NG setup between AMF and gNB. • Register the UE with 5G core • Establish a PDU session • When a PDU Session is established for a user or device, the PCF is notified and is responsible for determining the appropriate QoS parameters for the session's packet traffic. Response: • PCF has controlled the QoS for the packet traffic of the PDU Session.
6. Test Limits	NA
7. Expected Results	PCF should control the QoS for the packet traffic of the PDU Session.

1.Test No	GR_TSTP_3.8.1_A8
2. Test Details	Mechanism to initiate QoS Flow establishment and modification as part of the QoS control;.
3. Test Instruments Required	Wireshark, UE + gNB simulator tool
4. Test Setup	UE + gNB simulator tool, AMF, SMF, UPF, UDM, AUSF, UDR, NRF, PCF, NEF, NSSF, BSF
5. Test Procedure	Action • Establish NG setup between AMF and gNB. • Register the UE with 5G core • Establish a PDU session • When a PDU (Packet Data Unit) Session is established, the PCF, working in coordination with the SMF and other functions, determines the initial QoS requirements for the session. Based on subscriber profiles, service agreements, and network conditions, the PCF defines the QoS parameters such as data rate, latency, packet loss tolerance, and priority for the initial QoS flow. Response: • To initiate or modify QoS flows, signaling messages are exchanged between the PCF, SMF, and other related functions. The PCF communicates the QoS parameters and requirements to the SMF, which then configures the UPF and other relevant elements accordingly.
6. Test Limits	NA
7. Expected Results	PCF should perform the QoS Flow establishment and modification as part of the QoS control.

1.Test No	GR_TSTP_3.8.1_B
2. Test Details	Handling QoS Flows that require a guaranteed bitrate (GBR bearers) and QoS Flows for which there is no guaranteed bitrate (non-GBR bearers).
3. Test Instruments Required	Wireshark, UE + gNB simulator tool
4. Test Setup	UE + gNB simulator tool, AMF, SMF, UPF, UDM, AUSF, UDR, NRF, PCF, NEF, NSSF, BSF
5. Test Procedure	Action • Establish NG setup between AMF and gNB. • Register the UE with 5G core • Establish a PDU session • The Policy Control Function (PCF) enforces policies that guarantee the minimum data rate for GBR bearers. The PCF coordinates with the SMF to ensure that the UPF allocates sufficient resources to meet the guaranteed data rate. • The PCF and SMF work together to allocate resources based on policy rules, network conditions, and user subscription profiles for Non-GBR bearers. During congestion, resources might be shared among non-GBR bearers based on factors like priority and usage patterns. Response: • PCF is able to handle the QoS flows for GBR bearers and Non-GBR bearers..
6. Test Limits	NA
7. Expected Results	PCF is able to handle the QoS flows for GBR bearers and Non-GBR bearers.

1.Test No	GR_TSTP_3.8.1_C1
2. Test Details	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. Test Instruments Required	Wireshark, UE + gNB simulator tool
4. Test Setup	UE + gNB simulator tool, AMF, SMF, UPF, UDM, AUSF, UDR, NRF, PCF, NEF, NSSF, BSF
5. Test Procedure	Action • An emergency DNN is a special DNN associated with emergency services, such as police, fire, medical, or other critical services. When a UE's IP address belongs to an emergency DNN, it indicates that the UE is seeking emergency connectivity. • When the PCF receives a request from a UE with an IP address belonging to an emergency DNN, it directly uses the locally configured operator policies to make authorization and policy decisions. The PCF doesn't need to perform a subscription check because the priority is to provide emergency services promptly. Response: • The PCF has ensured that the UE's emergency service receives the appropriate QoS, priority, and resources as defined in the operator policies.
6. Test Limits	NA
7. Expected Results	The PCF should ensure that the UE's emergency service receives the appropriate QoS, priority, and resources as defined in the operator policies.

1.Test No	GR_TSTP_3.8.1_C2
2. Test Details	Charging control, policy control or both for a DNN access
3. Test Instruments Required	Wireshark, UE + gNB simulator tool
4. Test Setup	UE + gNB simulator tool, AMF, SMF, UPF, UDM, AUSF, UDR, NRF, PCF, NEF, NSSF, BSF
5. Test Procedure	Action • The Charging Control function involves monitoring and managing the charging aspects of network usage. For a specific DNN access, the PCF ensures that charging rules associated with that DNN are enforced. • The Policy Control function involves enforcing policies that govern how network resources are allocated and how services are treated. The PCF ensures that the QoS policies associated with a particular DNN are applied. This includes parameters like data rate, latency, priority, and handling of different types of traffic. Response: • PCF performs both Charging Control and Policy Control functions for a DNN access. It ensures that users receive the appropriate QoS, and their network usage is accurately charged based on the services they access through that DNN.
6. Test Limits	NA
7. Expected Results	PCF should perform both Charging Control and Policy Control functions for a DNN access. It ensures that users receive the appropriate QoS, and their network usage is accurately charged based on the services they access through that DNN.

1.Test No	GR_TSTP_3.8.1_C3
2. Test Details	Session management related functionality of Policy and charging control for a service data flow;
3. Test Instruments Required	Wireshark, UE + gNB simulator tool
4. Test Setup	UE + gNB simulator tool, AMF, SMF, UPF, UDM, AUSF, UDR, NRF, PCF, NEF, NSSF, BSF
5. Test Procedure	Action The PCRF is responsible for defining and distributing policy and charging rules to the PCF and CCF. • The PCF is responsible for enforcing policy rules that define how network resources are allocated and how services are treated. Response: • PCF has been enforced the policy and charging control rules for service data flow.
6. Test Limits	NA
7. Expected Results	PCF should enforce the policy and charging control rules for service data flow.

1.Test No	GR_TSTP_3.8.1_C4
2. Test Details	Selective Blocking of RCS Services based on PLMN, TAI and Postpaid/Prepaid Subscription.
3. Test Instruments Required	Wireshark, UE + gNB simulator tool
4. Test Setup	UE + gNB simulator tool, AMF, SMF, UPF, UDM, AUSF, UDR, NRF, PCF, NEF, NSSF, BSF
5. Test Procedure	Action • Selective blocking of Rich Communication Services (RCS) based on PLMN (Public Land Mobile Network), TAI (Tracking Area Identity), and subscription type (postpaid/prepaid) involves controlling access to specific RCS services for users based on various criteria. RCS services encompass enhanced messaging features like chat, file sharing, video calling, and more. Response: • Operators has been configured their networks to selectively block RCS services based on PLMN and TAI.
6. Test Limits	NA
7. Expected Results	Operators should configure their networks to selectively block RCS services based on PLMN and TAI.

1.Test No	GR_TSTP_3.8.1_C5
2. Test Details	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.
3. Test Instruments Required	Wireshark, UE + gNB simulator tool
4. Test Setup	UE + gNB simulator tool, AMF, SMF, UPF, UDM, AUSF, UDR, NRF, PCF, NEF, NSSF, BSF
5. Test Procedure	Action • The revalidationTime attribute specifies the time after which the policy decision needs to be revalidated. It defines the duration for which the policy decision remains valid without needing reevaluation. • The policyCtrlReqTriggers attribute specifies triggers that instruct the SMF to interact with the Policy Control Function (PCF) to request Policy and Charging Control (PCC) rules. Response: • By receiving the SmPolicyDecision data structure, SMF has sent a PCF interaction request to the PCF for the PCC rules.
6. Test Limits	NA
7. Expected Results	By receiving the SmPolicyDecision data structure, SMF should sent a PCF interaction request to the PCF for the PCC rules.

1.Test No	GR_TSTP_3.8.1_C6
2. Test Details	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.
3. Test Instruments Required	Wireshark, UE + gNB simulator tool
4. Test Setup	UE + gNB simulator tool, AMF, SMF, UPF, UDM, AUSF, UDR, NRF, PCF, NEF, NSSF, BSF
5. Test Procedure	Action • The revalidationTime attribute specifies the time after which the policy decision needs to be revalidated. It defines the duration for which the policy decision remains valid without needing reevaluation. • The policyCtrlReqTriggers attribute specifies triggers that instruct the SMF to interact with the Policy Control Function (PCF) to request Policy and Charging Control (PCC) rules. Response: • By receiving the SmPolicyDecision data structure, SMF has sent a PCF interaction request to the PCF for the PCC rules.
6. Test Limits	NA
7. Expected Results	By receiving the SmPolicyDecision data structure, SMF should sent a PCF interaction request to the PCF for the PCC rules.

1.Test No	GR_TSTP_3.8.1_C7
2. Test Details	Session binding, which shall take the following IP CAN parameters into account: (I) The UE IPv4 address and/or IPv6 network prefix; (II) The UE identity, if present; and The information about the packet data network (PDF) the user is
3. Test Instruments Required	Wireshark, UE + gNB simulator tool
4. Test Setup	UE + gNB simulator tool, AMF, SMF, UPF, UDM, AUSF, UDR, NRF, PCF, NEF, NSSF, BSF
5. Test Procedure	Action • When a user initiates a session, the network elements involved in session management, such as the SMF, use the IP CAN parameters to identify the user and the context of the session. • The SMF or relevant network element compares the provided IP CAN parameters (UE IP address, UE identity, PDN information) with the stored session context. Response: • The session has properly bounded to the user's session context after the IP CAN parameters matched the stored session context. This binding ensures that data traffic from the UE is routed correctly and receives the appropriate QoS and policies.
6. Test Limits	NA
7. Expected Results	If the IP CAN parameters match the stored session context, the session should properly bound to the user's session context.

1.Test No	GR_TSTP_3.8.1_C8
2. Test Details	Data barring based on PLMN and TAC (Type allocation code in IMEI);
3. Test Instruments Required	Wireshark, UE + gNB simulator tool
4. Test Setup	UE + gNB simulator tool, AMF, SMF, UPF, UDM, AUSF, UDR, NRF, PCF, NEF, NSSF, BSF
5. Test Procedure	Action • Data barring based on PLMN (Public Land Mobile Network) and TAC (Type Allocation Code) is a network functionality that allows a mobile network operator to restrict or block data services for specific devices or users based on their location (PLMN) and the Type Allocation Code (TAC) found in the International Mobile Equipment Identity (IMEI) of the device. Response: • Network operator has been enforced the data barring rules for the User based on the PLMN and TAC.
6. Test Limits	NA
7. Expected Results	Network operator should enforce the data barring rules for the User based on the PLMN and TAC.

1.Test No	GR_TSTP_3.8.1_C9
2. Test Details	Modification of the authorized Session AMBR at any time during the lifetime of the PDU session and provision it to the SMF;
3. Test Instruments Required	Wireshark, UE + gNB simulator tool
4. Test Setup	UE + gNB simulator tool, AMF, SMF, UPF, UDM, AUSF, UDR, NRF, PCF, NEF, NSSF, BSF
5. Test Procedure	Action • Establish NG setup between AMF and gNB. • Register the UE with 5G core • Establish a PDU session. • The PCF defines the authorized Session AMBR PDU session when is established. The authorized Session AMBR sets the upper limit for the combined uplink and downlink data rates for the session. • Throughout the lifetime of the PDU session, the PCF monitors network conditions, congestion levels, and user behavior. Based on these factors, the PCF may decide to modify the authorized Session AMBR to better allocate network resources. Response: • Once the PCF decides to modify the authorized Session AMBR, it communicates this modification to the SMF. The PCF provides the updated AMBR values and reasons for the modification.
6. Test Limits	NA
7. Expected Results	PCF should send the updated AMBR values and reasons for the modification to the SMF.

1.Test No	GR_TSTP_3.8.1_C10
2. Test Details	Modification of the authorized Default QoS during the lifetime of the PDU session and provision it to the SMF.
3. Test Instruments Required	Wireshark, UE + gNB simulator tool
4. Test Setup	UE + gNB simulator tool, AMF, SMF, UPF, UDM, AUSF, UDR, NRF, PCF, NEF, NSSF, BSF
5. Test Procedure	Action • Establish NG setup between AMF and gNB. • Register the UE with 5G core • Establish a PDU session • When a user initiates a PDU session or an existing session is established, the PCF determines the authorized Default QoS based on the user's subscription profile, service agreements, and network policies. • The PCF communicates with the SMF to provision the authorized Default QoS parameters for the PDU session. The SMF configures the User Plane Function (UPF) and other relevant network elements to adhere to the authorized Default QoS. Response: • The PCF has communicated with the SMF to provision the authorized Default QoS parameters for the PDU session.
6. Test Limits	NA
7. Expected Results	The PCF should communicate with the SMF to provision the authorized Default QoS parameters for the PDU session

1.Test No	GR_TSTP_3.8.1_C11
2. Test Details	Roaming - Communication with H-PCF over N24 interface for obtaining relevant UE Policy via SEPP.
3. Test Instruments Required	Wireshark, UE + gNB simulator tool
4. Test Setup	UE + gNB simulator tool, AMF, SMF, UPF, UDM, AUSF, UDR, NRF, PCF, NEF, NSSF, BSF
5. Test Procedure	**Action:** • UE registers in V-PLMN and establishes a PDU session. • V-PCF requests UE policy information from H-PCF over **N24 via SEPP**. • H-PCF returns policy rules (QoS, charging, access restrictions) to V-PCF. • SMF enforces received policy for the UE session. • Capture N24 and SEPP signaling using Wireshark. **Response:** • H-PCF successfully provides UE policy to V-PCF. • SMF enforces policy in visited network. • SEPP securely routes requests and responses between V-PCF and H-PCF.
6. Test Limits	NA
7. Expected Results	• Communication over **N24 via SEPP** is successfully established. • V-PCF receives correct UE policy from H-PCF. • Policy enforcement in V-PLMN occurs as per H-PCF directives. • Wireshark traces confirm proper **N24 and SEPP signaling** and secure routing.

1.Test No	GR_TSTP_3.9.1_A
2. Test Details	NEF shall be connected with other 3GPP network elements using standard Service based interface (a) NRF; (b) UDR, N37; (c) BSF; (d) PCF, N30; and (e) AF, N33
3. Test Instruments Required	Wireshark, UE + gNB simulator tool
4. Test Setup	UE + gNB simulator tool, AMF, SMF, UPF, UDM, AUSF, UDR, NRF, PCF, NEF, NSSF, BSF
5. Test Procedure	Action • NEF triggered traffic steering routing with the AF. (Based on slice,Dnn,Supi,Gpsi). • Nef retrieval policies from PCF. • BSF provides events to NEF for allowing external applications to securely interact with the policy framework for policy control to 3GPP network Response: • NEF has performed the scenarios mentioned in the action section.
6. Test Limits	NA
7. Expected Results	NEF should communicate with NRF, UDR, BSF, PCF and AF based on SBI architecture

1.Test No	GR_TSTP_3.9.1_B
2. Test Details	The NEF shall support following services: Service-based interface Nnef;
3. Test Instruments Required	Wireshark, UE + gNB simulator tool
4. Test Setup	UE + gNB simulator tool, AMF, SMF, UPF, UDM, AUSF, UDR, NRF, PCF, NEF, NSSF, BSF
5. Test Procedure	Action • The NEF exposes various network services, such as data services, voice services, IoT services, etc., to external applications and services • The NEF manages the interactions between external applications and the network services Response: • The Network Exposure Function (NEF) is a component in 5G networks responsible for exposing and managing network services to external applications
6. Test Limits	NA
7. Expected Results	NEF should be responsible for exposing and managing network services to external applications

1.Test No	GR_TSTP_3.9.1_C1
2. Test Details	The NEF shall support: Masking of network and user sensitive information to external AF's according to the network policy.
3. Test Instruments Required	Wireshark, UE + gNB simulator tool
4. Test Setup	UE + gNB simulator tool, AMF, SMF, UPF, UDM, AUSF, UDR, NRF, PCF, NEF, NSSF, BSF
5. Test Procedure	Action • The NEF identifies sensitive information within the data that is being exposed to external AFs. This could include personally identifiable information (PII), network configuration details, user identities, and more. Response: • NEF is using security policy if any external AF request
6. Test Limits	NA
7. Expected Results	NEF should use security policy if any external AF request

1.Test No	GR_TSTP_3.9.1_C2
2. Test Details	Procedure for resource management of Background Data Transfer (BDT)
3. Test Instruments Required	Wireshark, UE + gNB simulator tool
4. Test Setup	UE + gNB simulator tool, AMF, SMF, UPF, UDM, AUSF, UDR, NRF, PCF, NEF, NSSF, BSF
5. Test Procedure	Action • An external application or service initiates a request for a background data transfer through the NEF. The BDT request includes details such as the nature of the data, desired transfer rate, and any QoS (Quality of Service) requirements. Response: • NEF is using UDM/UDR to get any information about you
6. Test Limits	NA
7. Expected Results	NEF should use UDM/UDR to get any information about you

1.Test No	GR_TSTP_3.9.1_C3
2. Test Details	Resource Management of BDT API for background data transfer.
3. Test Instruments Required	Wireshark, UE + gNB simulator tool
4. Test Setup	UE + gNB simulator tool, AMF, SMF, UPF, UDM, AUSF, UDR, NRF, PCF, NEF, NSSF, BSF
5. Test Procedure	Action • An external application or service initiates a request for a background data transfer through the NEF. The BDT request includes details such as the nature of the data, desired transfer rate, and any QoS (Quality of Service) requirements. Response: • NEF is using UDM/UDR to get any information about you
6. Test Limits	NA
7. Expected Results	NEF should use UDM/UDR to get any information about you

1.Test No	GR_TSTP_3.9.1_C4
2. Test Details	Nnef_TrafficInfluence service, Nnef_AFsessionWithQoS service
3. Test Instruments Required	Wireshark, UE + gNB simulator tool
4. Test Setup	UE + gNB simulator tool, AMF, SMF, UPF, UDM, AUSF, UDR, NRF, PCF, NEF, NSSF, BSF
5. Test Procedure	Action • Nnef_TrafficInfluence service could be related to influencing or managing the traffic behavior within the network. • BDTP likely stands for "Bearer Determination and Traffic Policing." This service might involve the negotiation and management of bearer contexts for different types of network traffic. • Nnef_ChargeableParty service This service could be related to managing and identifying the chargeable party for network services or transactions. • Nnef_AFsessionWithQoS service likely involves establishing sessions for specific applications with defined Quality of Service (QoS) parameters. Response: • NEF can support the all above mentioned services.
6. Test Limits	NA
7. Expected Results	NEF should support the all above mentioned services.

1.Test No	GR_TSTP_3.9.1_C5
2. Test Details	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
3. Test Instruments Required	Wireshark, UE + gNB simulator tool
4. Test Setup	UE + gNB simulator tool, AMF, SMF, UPF, UDM, AUSF, UDR, NRF, PCF, NEF, NSSF, BSF
5. Test Procedure	Action • Establish NG setup between AMF and gNB. • Register the UE with 5G core • PDU session establishment • PDU session modification Response: • NEF is supporting all security capability and exposure capability
6. Test Limits	NA
7. Expected Results	NEF should support all security capability and exposure capability

1.Test No	GR_TSTP_3.9.1_C6
2. Test Details	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.
3. Test Instruments Required	Wireshark, UE + gNB simulator tool
4. Test Setup	UE + gNB simulator tool, AMF, SMF, UPF, UDM, AUSF, UDR, NRF, PCF, NEF, NSSF, BSF
5. Test Procedure	Action • NF's send POST /nudm-sdm/v2/imsi-311480110000001 Response: • NEF send 200 0k
6. Test Limits	NA
7. Expected Results	NEF should send 200 0k

1.Test No	GR_TSTP_3.9.1_C7
2. Test Details	Nnef_BDTPNegotiation service, Nnef_ChargeableParty service, NF_management operations with NRF, exposure of bulk subscription.
3. Test Instruments Required	Wireshark, UE + gNB simulator tool
4. Test Setup	UE + gNB simulator tool, AMF, SMF, UPF, UDM, AUSF, UDR, NRF, PCF, NEF, NSSF, BSF
5. Test Procedure	Action • Nnef_TrafficInfluence service could be related to influencing or managing the traffic behavior within the network. • BDTP likely stands for "Bearer Determination and Traffic Policing." This service might involve the negotiation and management of bearer contexts for different types of network traffic. • Nnef_ChargeableParty service This service could be related to managing and identifying the chargeable party for network services or transactions. • Nnef_AFsessionWithQoS service likely involves establishing sessions for specific applications with defined Quality of Service (QoS) parameters. Response: • NEF can support the all above mentioned services.
6. Test Limits	NA
7. Expected Results	NEF should support the all above mentioned services.

1.Test No	GR_TSTP_3.9.1_C8
2. Test Details	Translatation of information exchanged with the AF and information exchanged with the internal network function.
3. Test Instruments Required	Wireshark, UE + gNB simulator tool
4. Test Setup	UE + gNB simulator tool, AMF, SMF, UPF, UDM, AUSF, UDR, NRF, PCF, NEF, NSSF, BSF
5. Test Procedure	Action • External AFs and internal NFs might use different communication protocols or data formats. The NEF performs protocol translation to convert data from the format used by the AF to the format understood by the internal NF, and vice versa. Response: • The NEF's translation capabilities ensure that both external AFs and internal NFs can interact efficiently, even if they
6. Test Limits	NA
7. Expected Results	NEF will Translate of information exchanged with the AF and information exchanged with the internal network function

1.Test No	GR_TSTP_3.9.1_D
2. Test Details	NEF may be connected to UDR, using standard Service based interface N37.
3. Test Instruments Required	Wireshark, UE + gNB simulator tool
4. Test Setup	UE + gNB simulator tool, AMF, SMF, UPF, UDM, AUSF, UDR, NRF, PCF, NEF, NSSF, BSF
5. Test Procedure	**Action:** • NEF initiates a service request to UDR over **N37**. • UDR responds with requested subscriber/policy data. • Capture N37 signaling using Wireshark. **Response:** • UDR successfully returns requested data to NEF. • NEF processes retrieved information for exposure services. • Correct SB interface interactions observed.
6. Test Limits	NA
7. Expected Results	• NEF successfully connects to UDR over **N37**. • Data retrieved from UDR matches expected subscriber/policy information. • Signaling traces confirm correct **NEF ↔ UDR** communication via N37.

1.Test No	GR_TSTP_3.10.1_A
2. Test Details	Verify that NSSF shall be connected with other 3GPP network elements, viz. NRF and AMF, using Standard Service-based Interface.
3. Test Instruments Required	Wireshark, UE + gNB simulator tool
4. Test Setup	Test Setup Small size 5G Core-1
5. Test Procedure	Action • Establish NG setup between AMF and gNB. • Register the UE with 5G core • NSSF and NRF, AMF, configurations and interface details are available • The 5G network environment with functional NSSF and NRF, AMF instances is set up. Response: • Messages should be exchange Successful between NSSF and NRF, AMF, via the interface
6. Test Limits	NA
7. Expected Results	NRF send 201 ok. The NSSF successfully establishes a connection with the NRF, AMF using the standard service-based interface.

<table>
<tr><td>1.Test No</td><td>GR_TSTP_3.10.1_B</td></tr>
<tr><td>2. Test Details</td><td>NSSF may be connected with other 3GPP network elements, viz. EMS using Standard Service-based Interface</td></tr>
<tr><td>3. Test Instruments Required</td><td>Wireshark, UE + gNB simulator tool</td></tr>
<tr><td>4. Test Setup</td><td>Test Setup Small size 5G Core-1</td></tr>
<tr><td>5. Test Procedure</td><td>Action
• Establish NG setup between AMF and gNB.
• Register the UE with 5G core
• NSSF and EMS configurations and interface details are available
• The 5G network environment with functional NSSF and EMS instances is set up.
Response:
• Messages should be exchange Successful between NSSF EMS via the interface</td></tr>
<tr><td>6. Test Limits</td><td>NA</td></tr>
<tr><td>7. Expected Results</td><td>NRF send 201 ok.
The NSSF successfully establishes a connection with the EMS using the standard service-based interface.</td></tr>
</table>

1.Test No	GR_TSTP_3.10.1_C1
2. Test Details	Verify that Determination of the Allowed NSSAI.
3. Test Instruments Required	Wireshark, UE + gNB simulator tool
4. Test Setup	Test Setup Small size 5G Core-1
5. Test Procedure	Action • Establish NG setup between AMF and gNB. • Register the UE with 5G core • The UE initiates a request to the NSSF for determining the AMF set to serve it. • The request may include UE identity, location, requested services, and other relevant parameters. Response: • The NSSF processes the request and determines the appropriate AMF set to serve the UE.
6. Test Limits	NA
7. Expected Results	NRF send 201 ok. ""targetAmfSet"":""311-480-ca-3ff. The UE should be receiving the information about the selected AMF set from the NSSF

1.Test No	GR_TSTP_3.10.1_C2
2. Test Details	Verify that Single UE access to one or more Network Slice Instance
3. Test Instruments Required	Wireshark, UE + gNB simulator tool
4. Test Setup	Test Setup Small size 5G Core-1
5. Test Procedure	Action • Establish NG setup between AMF and gNB. • The 5G network infrastructure with properly configured NSSIs and NSSIs. • The UE capable of connecting to the 5G network. • The single UE initiates a request to access a specific Network Slice • Instance. • The allocated resources match the defined QoS for the slice. Response: Response: • The UE successfully accesses and uses resources from one and multiple Network Slice Instances simultaneously
6. Test Limits	NA
7. Expected Results	"NSSF send 200 ok {""allowedSnssaiList"":[{""allowedSnssai"":{""sst"":1,""sd"":""0000d1""}} "

1.Test No	GR_TSTP_3.10.1_C3
2. Test Details	Verify that Selection of same AMF for different set of slices.
3. Test Instruments Required	Wireshark, UE + gNB simulator tool
4. Test Setup	Test Setup Small size 5G Core-1
5. Test Procedure	Action • Establish NG setup between AMF and gNB. • Register the UE with 5G core. • The 5G network infrastructure with support for network slicing is set up. • Network receives slice activation requests for different sets of slices (SNSSAIs) from multiple UE. • The same AMF instance is assigned to manage devices across both network slices. Response: • Devices should be different network slices can successfully register with the same AMF.
6. Test Limits	NA
7. Expected Results	UEs using different sets of slices are successfully connected to the same AMF

1.Test No	GR_TSTP_3.10.1_C4
2. Test Details	Nnssf_NSSelection for slice-info-request-for-registration to provide the Allowed NSSAI, configured NSSAI and may provide AMF set or the list of candidate AMF information to the Requester in Roaming scenarios and, if needed, mapping to the Subscribed S-NSSAIs.
3. Test Instruments Required	Wireshark, UE + gNB simulator tool
4. Test Setup	Test Setup Small size 5G Core-1
5. Test Procedure	Action • Register the UE with 5G core • The AMF in the visited PLMN receives a request to initiate network registration for a roaming UE. • The AMF queries the Nnssf_NSSelection service for slice information using the "slice-info-request-for-registration" indication. • The Nnssf_NSSelection service gathers Allowed NSSAI, configured NSSAI, AMF set, and potentially mapped Subscribed S-NSSAIs. Response: • The Nnssf Successfully accurately determines the Allowed NSSAIs based on the roaming device's subscription profile. • NSSF send 200 ok
6. Test Limits	NA
7. Expected Results	"NSSF send 200 ok. {""allowedNssaiList"":[{""allowedSnssaiList"":[{""allowedSnssai"":{""sst"":1,""sd"":" "0000d1""}}],""accessType"":""3GPP_ACCESS""}],""targetAmfSet"":""311-480-ca3ff"",""nsiInformation"":{""nrfId"":""http://nrf-service:10500""}}" The AMF in the visited PLMN successfully receives the necessary slice information from the Nnssf_NSSelection service.

1.Test No	GR_TSTP_3.10.1_C5
2. Test Details	Provision of configured slice information for the PLMN when requested with "default configured S-NSSAI "indication.
3. Test Instruments Required	Wireshark, UE + gNB simulator tool
4. Test Setup	Test Setup Small size 5G Core-1
5. Test Procedure	Action • Register the UE with 5G core • The NSSF processes the query and identifies that the requester is seeking default configured slice information for the PLMN. • PLMN configurations and slice profiles are available. • The PLMN supports NSSAI and has configured slice information Response: • The NSSF responds to the initiator with the configuration information for the default configured S-NSSAI(s) for the PLMN.
6. Test Limits	NA
7. Expected Results	The NSSF successfully provides the queried default configured slice information for the PLMN.

1.Test No	GR_TSTP_3.10.1_C6
2. Test Details	Availability Service to provide AuthorizedNssaiAvailabilityInfo slice that is available per TAI for the S-NSSAIs the NF service consumer supports
3. Test Instruments Required	Wireshark, UE + gNB simulator tool
4. Test Setup	Test Setup Small size 5G Core-1
5. Test Procedure	Action • Register the UE with 5G core • The NF service consumer is registered and authorized to use the Availability Service. • Availability Service and NF service consumer are up and running. Response: • NSSF send 200 ok • The response contains the AuthorizedNssaiAvailabilityInfo organized per TAI.
6. Test Limits	NA
7. Expected Results	"NSSF send 200 ok {""allowedNssaiList"":[{""allowedSnssaiList"":[{""allowedSnssai"":{""sst"":1,""sd"":" "0000d1""}}],""accessType"":""3GPP_ACCESS""}]"

1.Test No	GR_TSTP_3.10.1_C7
2. Test Details	Following services: (IV) NFRegister service; (V) NFDeregister service; and (VI) NFStatusNotify service.
3. Test Instruments Required	Wireshark, UE + gNB simulator tool
4. Test Setup	Test Setup Small size 5G Core-1
5. Test Procedure	Action • Register the UE with 5G core • A 5G network environment with functional NFRegister service and supporting components is set up. • Registered NF instances and deregistration configurations are available. Response: • The NF successfully registers and deregisters from the network, and any necessary cleanup is completed.
6. Test Limits	NA
7. Expected Results	1.The NFRegister service successfully processes the registration request. 2.The NFDeregister service successfully processes the deregistration request. 3.The NFStatusNotify service successfully processes the status notification request..

1.Test No	GR_TSTP_3.10.1_D
2. Test Details	The NSSF may support following services: (III) NFStatusSubscribe service; and (IV) NFProfileRetrieval service
3. Test Instruments Required	Wireshark, UE + gNB simulator tool
4. Test Setup	Test Setup Small size 5G Core-1
5. Test Procedure	Action • Establish NG setup between AMF and gNB. • Register the UE with 5G core • The 5g network environment with a functional NFStatusSubscribe service and supporting components is set up. • NF instances, status notification configurations, and subscriber information are available Response: • The subscriber is correctly registered for status notifications and associated with the specified NF instances.
6. Test Limits	NA
7. Expected Results	The NFStatusSubscribe service successfully processes the subscription request.

1.Test No	GR_TSTP_3.10.1_E1
2. Test Details	Nnssf_NSSAIAvailability delete service operation for deletion of availability of S-NSSAIs per TA.
3. Test Instruments Required	Wireshark, UE + gNB simulator tool
4. Test Setup	Test Setup Small size 5G Core-1
5. Test Procedure	Action • Register the UE with 5G core • The NSSF processes the request and identifies the relevant S-NSSAIs and TA for deletion. • The NSSF removes the availability information of the specified S-NSSAIs within the given TA. Response: • The NSSF responds to the initiator indicating the successful deletion of the availability information for the specified S-NSSAIs within the TA.
6. Test Limits	NA
7. Expected Results	The availability information for the specified S-NSSAIs within the TA has been successfully deleted from the NSSF's records.

1.Test No	GR_TSTP_3.10.1_E2
2. Test Details	NSSF shall have capability to provide bulk provisioning over all exposed interfaces. It shall provide Real time subscriber data synchronization.
3. Test Instruments Required	Wireshark, UE + gNB simulator tool
4. Test Setup	Test Setup Small size 5G Core-1
5. Test Procedure	Action • Establish NG setup between AMF and gNB. • Register the UE with 5G core • The NSSF instance with support for bulk provisioning is set up Response: • The NSSF successfully processes the bulk provisioning request without errors.
6. Test Limits	NA
7. Expected Results	NSSF send 201 ok Created targetAmfSet"":""311-480-ca-3ff"""

1.Test No	GR_TSTP_3.10.1_E3
2. Test Details	Roaming - Communication with the H-NSSF for selection of the S-NSSAI applicable in the case of roaming.
3. Test Instruments Required	Wireshark, UE + gNB simulator tool
4. Test Setup	Test Setup Small size 5G Core-1
5. Test Procedure	**Action:** • UE registers in V-PLMN and requests PDU session in a specific slice. • V-AMF queries H-NSSF to determine applicable **S-NSSAI** for the UE. • H-NSSF responds with authorized slice(s) and related parameters. • V-AMF assigns S-NSSAI to UE session and configures SMF accordingly. • Capture signaling between V-AMF ↔ H-NSSF (via N33/N32 or SEPP) using Wireshark. **Response:** • H-NSSF returns correct S-NSSAI information. • V-PLMN assigns slice(s) consistent with home subscription. • Signaling shows secure inter-PLMN communication and correct S-NSSAI mapping.
6. Test Limits	NA
7. Expected Results	• Communication with H-NSSF successfully resolves UE's **S-NSSAI** for roaming. • UE PDU session is established with correct network slice in visited PLMN. • Signaling traces confirm proper **V-AMF** ↔ **H-NSSF** interaction and slice selection per **3GPP TS 23.501/TS 29.531**.

1.Test No	GR_TSTP_3.11.1_A
2. Test Details	The BSF shall be compliant with 3GPP TS 29.521 “Binding Support Management service”.
3. Test Instruments Required	Wireshark, UE + gNB simulator tool
4. Test Setup	Test Setup Small size 5G Core-1
5. Test Procedure	Action • Establish NG setup between AMF and gNB. • Register the UE with 5G core • PDU session establishment • PCF will send a request to store the binding information at the BSF Response: • BSF has been stored the binding information which is received from the PCF
6. Test Limits	N/A
7. Expected Results	BSF is using SBI architecture to communicate with PCF

1.Test No	GR_TSTP_3.11.1_B1
2. Test Details	Registration of BSF profile with NRF, if NRF is available/part of the 5G compact mobile system
3. Test Instruments Required	Wireshark, UE + gNB simulator tool
4. Test Setup	Test Setup Small size 5G Core-1
5. Test Procedure	Action • UE send PUT Request to NRF for register Response: • BSF registration has been successful in the NRF
6. Test Limits	N/A
7. Expected Results	NRF should send 201 Created to BSF

1.Test No	GR_TSTP_3.11.1_B2
2. Test Details	Heartbeat procedure periodically with NRF to update NF status. This heartbeat message shall also include BSF load information, if NRF is available/part of the 5G compact mobile system.
3. Test Instruments Required	Wireshark, UE + gNB simulator tool
4. Test Setup	Test Setup Small size 5G Core-1
5. Test Procedure	Action • BSF send PATCH heartbeat request after 60 sec to NRF Response: • BSF got the successful response from the NRF
6. Test Limits	N/A
7. Expected Results	NRF should send 204 to BSF

1.Test No	GR_TSTP_3.11.1_B3
2. Test Details	Discovery of BSF via Nnrf_Discovery API by the NF Consumers (NEF or AF), if NRF is available/part of the 5G compact mobile system.
3. Test Instruments Required	Wireshark, UE + gNB simulator tool
4. Test Setup	Test Setup Small size 5G Core-1
5. Test Procedure	Action • AF send Discovery request to NRF for BSF Response: • BSF has been discovered by NRF
6. Test Limits	N/A
7. Expected Results	NRF should send 200 Ok with BSF Data to AF

1.Test No	GR_TSTP_3.11.1_B4
2. Test Details	Creation, storage, updation and deletion of session binding information with various parameters such as UE address, PCF ID, DNN, SUPI or SNSSAI.
3. Test Instruments Required	Wireshark, UE + gNB simulator tool
4. Test Setup	Test Setup Small size 5G Core-1
5. Test Procedure	Action • BSF will perform creation, updating, and deletion of session binding information with various parameters such as UE address, PCF ID, DNN, SUPI or S-NSSAI. Response: • BSF has been performed the required methods
6. Test Limits	N/A
7. Expected Results	BSF should perform the required methods (creation, updating, and deletion of session binding information)

1.Test No	GR_TSTP_3.11.1_B5
2. Test Details	Binding between PCF and NEF or AF.
3. Test Instruments Required	Wireshark, UE + gNB simulator tool
4. Test Setup	Test Setup Small size 5G Core-1
5. Test Procedure	Action • When the PCF needs to communicate with the NEF or AF, the BSF comes into play to verify the identities and permissions of both the PCF and the NEF/AF. • The BSF provides security functions such as authentication, authorization, and key management to ensure the integrity and confidentiality of the communication. • The PCF initiates a binding request with the BSF, indicating its intention to communicate with the NEF or AF. The BSF verifies the identity of the PCF and ensures that it is authorized to interact with the NEF or AF. Response: • Once the verification is successful, the BSF has confirmed the binding between the PCF and the NEF or AF.
6. Test Limits	NA
7. Expected Results	Once the verification is successful, the BSF should confirm the binding between the PCF and the NEF or AF.

1.Test No	GR_TSTP_3.11.2_A1
2. Test Details	Use of Nbsf_Management_Register, Nbsf_Management_Deregister and Nbsf_Management_Update service operations by PCF;
3. Test Instruments Required	Wireshark, UE + gNB simulator tool
4. Test Setup	Test Setup Small size 5G Core-1
5. Test Procedure	Action • PCF will invoke into the Nbsf_Management_Register, Nbsf_Management_Deregister and Nbsf_Management_Update services to perform required operations. Response: • BSF has provided the successful responses to the PCF
6. Test Limits	NA
7. Expected Results	BSF should provide the successful responses to the PCF

1.Test No	GR_TSTP_3.11.2_A2
2. Test Details	Nbsf_Management_Register, Nbsf_Management_Deregister and, Nbsf_Management_Update to register, deregister and update binding information into the BSF
3. Test Instruments Required	Wireshark, UE + gNB simulator tool
4. Test Setup	Test Setup Small size 5G Core-1
5. Test Procedure	Action • PCF will invoke into the Nbsf_Management_Register, Nbsf_Management_Deregister and Nbsf_Management_Update services to register, deregister and update binding information into the BSF. Response: • BSF has successfully performed the required operations according to the PCF requests.
6. Test Limits	NA
7. Expected Results	BSF should provide the successful responses to the PCF

1.Test No	GR_TSTP_3.11.2_A3
2. Test Details	Use of Nbsf_Management_Deregister service operation to delete binding information when Policy Association Termination is initiated by the SMF and PCF.
3. Test Instruments Required	Wireshark, UE + gNB simulator tool
4. Test Setup	Test Setup Small size 5G Core-1
5. Test Procedure	Action • SMF and PCF will initiate the Policy Association Termination request. Response: • BSF has been deleted the binding information by invoking the Nbsf_Management_Deregister service operation.
6. Test Limits	NA
7. Expected Results	BSF should delete the binding information.

1.Test No	GR_TSTP_3.11.2_A4
2. Test Details	Use of Nbsf_Management_Deregister service operation to delete binding information when Policy Association Termination is initiated by the PCF.
3. Test Instruments Required	Wireshark, UE + gNB simulator tool
4. Test Setup	Test Setup Small size 5G Core-1
5. Test Procedure	Action • PCF will initiate the Policy Association Termination request. Response: • BSF has been deleted the binding information by invoking the Nbsf_Management_Deregister service operation.
6. Test Limits	NA
7. Expected Results	BSF should delete the binding information.

1.Test No	GR_TSTP_3.11.2_B1
2. Test Details	Use of Nbsf_Management_Discovery service operation to obtain the selected PCF id for a PDU session by a client NEF, NWDAF, AF, IMS, DRA). BSF responds with the PCF id and others related binding information.
3. Test Instruments Required	Wireshark, UE + gNB simulator tool
4. Test Setup	Test Setup Small size 5G Core-1
5. Test Procedure	Action • BSF gets the Nbsf_Management_Discovery service request by a clientNEF, NWDAF, AF, IMS, DRA) for selected PCF idfor a PDUsession Response: • BSF responds with the PCF id and others related binding information.
6. Test Limits	NA
7. Expected Results	BSF should responds with the PCF id and others related binding information

1.Test No	GR_TSTP_3.12.1_A1
2. Test Details	The CHF shall support: Following charging features: (VI) Usage based charging; VII) Speed based charging/ Quality of service charging; III) Application ID charging; (IX) Network slice-based charging on 5G; URL based charging.
3. Test Instruments Required	Wireshark, UE + gNB simulator tool
4. Test Setup	Test Setup Small size 5G Core-1
5. Test Procedure	Action • Trigger a usage event for a subscriber's data consumption. • Check if the CHF records the event and calculates the corresponding charges accurately. • Simulate different data sessions with varying speeds for a subscriber. • Ensure that the CHF correctly applies charges based on the speed/quality of service for each session. • Initiate data sessions using different applications (e.g., streaming, browsing, social media) for a subscriber. • Confirm that the CHF identifies the application IDs and applies appropriate charges according to predefined rules. • set up a 5G network slice with specific characteristics (e.g., bandwidth, latency). • Establish data connections within the network slice and observe if the CHF accurately charges based on slice attributes. • Access different URLs with varying data sizes for a subscriber's browsing session. • Check if the CHF identifies URLs and applies charges based on predefined URL charging rules. Response: • Core has been performed the initiated procedures
6. Test Limits	NA
7. Expected Results	• Usage event is recorded, and charges are calculated accurately. • Charges vary based on session speeds/quality of service as expected. • Charges reflect the correct application IDs associated with the data sessions. • Charges align with the network slice attributes for 5G connections. • Charges are appropriately categorized for video, HTTP, and WiFi usage. • Charges are applied according to the predefined charging rules for different URLs.

1.Test No	GR_TSTP_3.12.1_A2
2. Test Details	The CHF shall support: converged online charging and offline charging functionalities. The CHF provides the following: (I) Quota; (II) Re-authorization triggers; (III) Receiving service usage reports from NF Service Consumer; and (IV) CDRs generation.
3. Test Instruments Required	Wireshark, UE + gNB simulator tool
4. Test Setup	Test Setup Small size 5G Core-1
5. Test Procedure	Action • Initiate a session for a subscriber with defined quotas. • Verify that the CHF rejects the service initiation and notifies the NF Service Consumer about the quota exhaustion. • Initiate a session for a subscriber. • Verify that the CHF sends a re-authorization request to the relevant entities. • Simulate re-authorization success from external systems. • Verify that the CHF resumes or allows continued service usage. • Verify that the CHF accurately receives and processes the service usage reports. • Cross-check the received service usage reports with the internally maintained records in the CHF. • Verify that the CHF generates Call Detail Records (CDRs) for each completed session. • Inspect the generated CDRs for accuracy, including relevant information such as duration, timestamp, subscriber details, and consumed resources. Response: • Core has been performed the initiated procedures
6. Test Limits	NA
7. Expected Results	• The CHF should have accurately deducted and managed quotas during service usage. • Re-authorization triggers should lead to proper re-authorization and

	resumption of service. • The CHF should have received and processed service usage reports from the NF Service Consumer. • Accurate CDRs should be generated by the CHF for completed sessions.

1.Test No	GR_TSTP_3.12.1_A3
2. Test Details	N40 interface with the SMF for Data Connectivity Charging, which includes: (III) Flow based charging (FBC); and QoS Flow based Charging (QBC).
3. Test Instruments Required	Wireshark, UE + gNB simulator tool
4. Test Setup	Test Setup Small size 5G Core-1
5. Test Procedure	Action • Initiate a data session for a test subscriber. • Generate different types of traffic (e.g., HTTP, streaming, VoIP) during the session. • Monitor the N40 interface messages exchanged between CS and SMF. • Ensure that the CS correctly detects and categorizes different flows. • Verify that the CS applies appropriate charging rules for each flow type. • Check if the charging records for each flow are generated accurately. Response: • Core has been performed the initiated procedures
6. Test Limits	NA
7. Expected Results	The CS successfully detects and categorizes different flows, applies correct charging rules, and generates accurate charging records for each flow.

1.Test No	GR_TSTP_3.12.1_A4
2. Test Details	N40 interface with the SMF for Data Connectivity Charging, which includes: (I) Flow based charging (FBC); and QoS Flow based Charging (QBC).
3. Test Instruments Required	Wireshark, UE + gNB simulator tool
4. Test Setup	Test Setup Small size 5G Core-1
5. Test Procedure	Action • Trigger a time-based charging scenario for a subscriber's service usage. • Verify that the CHF system correctly calculates charges based on the duration of usage and the defined tariff rates. Verify that the CHF system consistently and accurately calculates charges based on the combined rules for each scenario. • Ensure that the calculated charges for each combination match the anticipated charges. Response: • Core has been performed the initiated procedures • All test scenarios have been executed successfully
6. Test Limits	NA
7. Expected Results	Check that the charges calculated match the expected charges for the specific event.

1.Test No	GR_TSTP_3.12.1_A5
2. Test Details	3GPP specified services;
3. Test Instruments Required	Wireshark, UE + gNB simulator tool
4. Test Setup	Test Setup Small size 5G Core-1
5. Test Procedure	Action • Verify Online Charging for Voice Call • Verify Offline Charging for Data Usage • Verify Charging for Supplementary Services • Verify Charging for Roaming Services Response: • Core has been performed the initiated procedures
6. Test Limits	NA
7. Expected Results	• Verify that the calculated charges match the expected charges for the supplementary service usage • Check that the calculated charges align with the expected charges for the roaming data services

1.Test No	GR_TSTP_3.12.1_A6
2. Test Details	Consumption of services exposed by the NRF;
3. Test Instruments Required	Wireshark, UE + gNB simulator tool
4. Test Setup	Test Setup Small size 5G Core-1
5. Test Procedure	Action • CHF should be able to register in NRF, re-register in NRF and able to communicate status of front end to NRF e.g., availability, load etc. • Validate that the retrieved tariff information matches the expected tariff rates for the service. • Trigger a request to obtain charging rules for a particular service or scenario from the NRF • Validate that the retrieved charging rules align with the expected rules for the specified service or scenario. Response: • Core has been performed the initiated procedures
6. Test Limits	NA
7. Expected Results	Validate that the retrieved subscriber profile information matches the expected profile data.

1.Test No	GR_TSTP_3.12.1_A7
2. Test Details	5G defined new identities: GPSI (MSISDN) and SUPI (IMSI);
3. Test Instruments Required	Wireshark, UE + gNB simulator tool
4. Test Setup	Test Setup Small size 5G Core-1
5. Test Procedure	Action • Verify Charging Using GPSI (MSISDN) • Confirm that the CHF system correctly identifies the subscriber based on the provided GPSI (MSISDN). • Verify Charging Using SUPI (IMSI) • Ensure that the CHF system correctly recognizes the subscriber based on the provided SUPI (IMSI). Response: • Core has been performed the initiated procedures
6. Test Limits	NA
7. Expected Results	• Validate that the calculated charges match the expected charges for the session. • Confirm that charges are calculated appropriately for the service session according to the defined tariff rates and session duration

1.Test No	GR_TSTP_3.12.1_A8
2. Test Details	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
3. Test Instruments Required	Wireshark, UE + gNB simulator tool
4. Test Setup	Test Setup Small size 5G Core-1
5. Test Procedure	Action • Verify Spending Limit Control with Multiple IP Addresses • Validate that the CHF system accurately tracks the usage across all IP addresses and enforces spending limits accordingly. • Verify Spending Limit Control with Multiple Slices • Confirm that the CHF system correctly attributes usage to the respective slices and enforces spending limits per slice. • Verify Spending Limit Control with Multiple Identifiers across Networks • Validate that the CHF system independently tracks usage and spending limits for each identifier. Response: • Core has been performed the initiated procedures
6. Test Limits	NA
7. Expected Results	• Verify that the system restricts further usage when the spending limit is reached. • Ensure that the subscriber is prevented from exceeding the spending limit for each slice. • Ensure that exceeding the spending limit for one identifier does not impact usage for others.

1.Test No	GR_TSTP_3.12.1_A9
2. Test Details	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;
3. Test Instruments Required	Wireshark, UE + gNB simulator tool
4. Test Setup	Test Setup Small size 5G Core-1
5. Test Procedure	Action • Verify CDR Generation and Storage • After each scenario, verify that the CHF system correctly generates a CDR based on the charging information. • Verify CDR Transfer Mechanism • Validate that the transferred CDRs retain their original format and integrity during the transfer process. • Verify CDR Parameter Description Response: • Core has performed the initiated procedures
6. Test Limits	NA
7. Expected Results	• Confirm that the generated CDRs are stored securely and accurately within the CHF system. • Verify that transferred CDRs are accurately received and stored in the external repository. • Ensure that each CDR parameter is correctly described and encoded according to the specified ASN.1 structure.

1.Test No	GR_TSTP_3.12.1_A10
2. Test Details	Upgradeability to 3GPP Rel-16 functionality and also backward compatibility;
3. Test Instruments Required	Wireshark, UE + gNB simulator tool
4. Test Setup	Test Setup Small size 5G Core-1
5. Test Procedure	Action • Verify Backward Compatibility • Validate that the CHF system behaves as expected and meets the specifications of the current 3GPP release • Upgrade to 3GPP Rel-16 Functionality • Verify that the CHF system correctly implements the new functionalities without impacting existing features. • Verify Coexistence of Rel-16 and pre-Rel-16 Functionalities • Confirm that the CHF system can seamlessly handle the coexistence of different functionalities. Response: • Core has performed the initiated procedures • Test report summarizing the outcomes of each test case.
6. Test Limits	NA
7. Expected Results	• Confirm that existing services, charging rules, and interfaces are functioning correctly. • Validate that the charging behavior aligns with 3GPP Release 16 specifications. • Validate that the system correctly applies the appropriate charging rules and behavior based on the scenario.

1.Test No	GR_TSTP_3.12.1_A11
2. Test Details	All mandatory fields for CDR in 3GPP TS32.255;
3. Test Instruments Required	Wireshark, UE + gNB simulator tool
4. Test Setup	Test Setup Small size 5G Core-1
5. Test Procedure	Action • Verify CDR Generation for Voice Call • Confirm that the CHF system generates a CDR with all the mandatory fields specified in 3GPP TS 32.255. • Verify CDR Generation for Data Usage • Confirm that the CHF system generates a CDR for the data session with all mandatory fields. • Verify CDR Generation for Supplementary Services • Verify that the CHF system generates a CDR with all mandatory fields to record the supplementary service usage. • Verify CDR Generation for Roaming Services • Confirm that the CHF system generates a CDR for the roaming data session, including all mandatory fields. Response: • Core has performed the initiated procedures
6. Test Limits	NA
7. Expected Results	• Validate that the CDR includes details such as calling and called party numbers, start time, duration, charging identifiers, etc. • Validate that the CDR contains information such as data volume, session start time, duration, charging identifiers, etc. • Validate that the CDR includes relevant details like the type of supplementary service, start time, duration, charging identifiers, etc. • Validate that the CDR includes details such as visited network identifier, data volume, session start time, duration, charging identifiers, etc.

1.Test No	GR_TSTP_3.12.1_A12
2. Test Details	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).
3. Test Instruments Required	Wireshark, UE + gNB simulator tool
4. Test Setup	Test Setup Small size 5G Core-1
5. Test Procedure	Action • Initiate Nchf_ConvergedCharging Request with MultipleUnitUsage • Initiate an Nchf_ConvergedCharging request containing MultipleUnitUsage information for the session • Process Charging Methods (Online and Offline) • If online charging is applicable, ensure that real-time charges are calculated and updated. • If offline charging is applicable, ensure that the charging data is recorded for later processing. • Generate MultipleUnitInformation in Response Response: • Core has performed the initiated procedures
6. Test Limits	NA
7. Expected Results	• Verify that the CHF system receives and correctly interprets the MultipleUnitUsage details for different Rating Groups. • Verify that the generated MultipleUnitInformation includes all relevant details specified in the 3GPP specifications.

1.Test No	GR_TSTP_3.12.1_A13
2. Test Details	Charging of roaming traffic.
3. Test Instruments Required	Wireshark, UE + gNB simulator tool
4. Test Setup	Test Setup Small size 5G Core-1
5. Test Procedure	Action • Initiate Roaming Data Session • Simulate a scenario where a subscriber is roaming in a foreign network and initiates a data session (e.g., web browsing). • Ensure that the roaming parameters are correctly configured and utilized for charging. • Verify Roaming Charging • Confirm that the CHF system correctly identifies the roaming usage and applies the relevant tariff rates defined in the roaming agreements. • Validate Charging Records • Verify that the CHF system generates charging records for the roaming data session Response: • Core has been performed the initiated procedures
6. Test Limits	NA
7. Expected Results	• Validate that the system calculates charges based on the data volume and the roaming tariff rates. • Ensure that the generated charging records include information such as visited network identifier, session start time, duration, data volume, tariff rates, and calculated charges.

1.Test No	GR_TSTP_3.12.1_A14 GR_TSTP_3.12.1_A15 GR_TSTP_3.12.1_A16
2. Test Details	Following interface functions from CHF perspective:
3. Test Instruments Required	Wireshark, UE + gNB simulator tool
4. Test Setup	Test Setup Small size 5G Core-1
5. Test Procedure	Action • CHF initiates a registration request with NRF • NRF sends a registration response to CHF • SMF initiates an update request with CHF. • CHF sends an update response to SMF. • CHF Registration/Update/Deregistration with NRF • CHF initiates a registration request with NRF. • NRF sends a registration response to CHF • NRF processes the deregistration request Response: • Core has performed the initiated procedures
6. Test Limits	NA
7. Expected Results	• CHF is registered with AMF, and a successful registration response is received. • CHF successfully updates information with SMF, and an update response is received. • CHF can successfully register, update, and deregister with NRF, and corresponding responses are received for each operation.

1.Test No	GR_TSTP_3.12.1_A17 GR_TSTP_3.12.1_A18 GR_TSTP_3.12.1_A19 GR_TSTP_3.12.1_A20
2. Test Details	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
3. Test Instruments Required	Wireshark, UE + gNB simulator tool
4. Test Setup	Test Setup Small size 5G Core-1
5. Test Procedure	Action • Verify Converged Charging Triggered by SMF • Simulate a data session triggered by the SMF for a subscriber • Verify Online Charging and Session Tracking • Validate that the CHF system performs online charging in real-time as per the defined tariff agreements. • Verify that the CHF system correctly tracks session-related details such as start time, session duration, data volume, etc • Verify Offline Charging and CDR Generation • After the session is completed, confirm that the CHF system generates offline charging records (CDRs) for the session. • Verify Notification Handling - Nchf_ConvergedCharging • Verify Notification Handling - Nchf_SpendingLimitControl_ Response: • Core has performed the initiated procedures
6. Test Limits	NA
7. Expected Results	• Validate that the CDRs include all relevant charging details as specified in the converged charging requirements. • Confirm that the notifications contain accurate information about the converged charging events. • Confirm that the notifications accurately convey the relevant spending control information.

1.Test No	GR_TSTP_3.12.1_A21
2. Test Details	Different charging between 4G and 5G.
3. Test Instruments Required	Wireshark, UE + gNB simulator tool
4. Test Setup	Test Setup Small size 5G Core-1
5. Test Procedure	Action • Initiate Data Session in 4G Network • Confirm that the CHF system identifies the network type as 4G and applies the corresponding tariff rates for charging. • Verify Charging for 5G Network • Validate that the CHF system calculates charges for the 5G data session based on the configured tariff rates for 5G services. Response: • Core has performed the initiated procedures
6. Test Limits	NA
7. Expected Results	• Ensure that the calculated charges match the expected charges for the 5G session • Ensure that the calculated charges align with the expected charges for the 4G session.

1.Test No	GR_TSTP_3.12.1_A21
2. Test Details	Different charging between 4G and 5G.
3. Test Instruments Required	Wireshark, UE + gNB simulator tool
4. Test Setup	Test Setup Small size 5G Core-1
5. Test Procedure	Action • Initiate Data Session in 4G Network • Confirm that the CHF system identifies the network type as 4G and applies the corresponding tariff rates for charging. • Verify Charging for 5G Network • Validate that the CHF system calculates charges for the 5G data session based on the configured tariff rates for 5G services. Response: • Core has performed the initiated procedures
6. Test Limits	NA
7. Expected Results	• Ensure that the calculated charges match the expected charges for the 5G session • Ensure that the calculated charges align with the expected charges for the 4G session.

1.Test No	GR_TSTP_3.12.1_B1
2. Test Details	Charging of 5G sessions in case of session and service continuity mode, as defined in TS 32.255.
3. Test Instruments Required	Wireshark, UE + gNB simulator tool
4. Test Setup	Test Setup Small size 5G Core-1
5. Test Procedure	Action • Verify Charging for Initial 5G Session • Validate that the CHF system calculates charges accurately for the initial 5G session based on the specified tariff rates. • Trigger Session Continuity • Simulate a session continuity event within the same 5G session. Response: • Core has performed the initiated procedures
6. Test Limits	NA
7. Expected Results	• Ensure that the calculated charges match the expected charges for the initial session • Confirm that the CHF system recognizes the session continuity and continues charging seamlessly

1.Test No	GR_TSTP_3.12.1_B2
2. Test Details	Spending Limit Control Service of the Nchf Service according to TS 32.290 and TS 29.504
3. Test Instruments Required	Wireshark, UE + gNB simulator tool
4. Test Setup	Test Setup Small size 5G Core-1
5. Test Procedure	Action • Verify Spending Limit Control with Multiple IP Addresses • Validate that the CHF system accurately tracks the usage across all IP addresses and enforces spending limits accordingly. • Verify Spending Limit Control with Multiple Slices • Confirm that the CHF system correctly attributes usage to the respective slices and enforces spending limits per slice. • Verify Spending Limit Control with Multiple Identifiers across Networks • Validate that the CHF system independently tracks usage and spending limits for each identifier. Response: • Core has been performed the initiated procedures
6. Test Limits	NA
7. Expected Results	• Verify that the system restricts further usage when the spending limit is reached. • Ensure that the subscriber is prevented from exceeding the spending limit for each slice. • Ensure that exceeding the spending limit for one identifier does not impact usage for others.

1.Test No	GR_TSTP_3.12.2_A1
2. Test Details	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).
3. Test Instruments Required	Wireshark, UE + gNB simulator tool
4. Test Setup	Test Setup Small size 5G Core-1
5. Test Procedure	Action • Verify QBC Charging for QoS Flows • Validate that the CHF system correctly tracks data volumes for each QoS flow associated with the session. • Validate Categorization by QoS Flow • Confirm that the CHF system categorizes the collected data volumes based on QFI, ensuring accurate attribution of charges. • Simulate Multiple PDU Sessions • Initiate multiple PDU sessions for the same subscriber, each with different QoS flows and QFIs. Response: • Core has performed the initiated procedures
6. Test Limits	NA
7. Expected Results	• Verify that the CHF system accurately applies the tariff rates defined for each QoS Flow Identifier (QFI) • Validate that the calculated charges for each QoS flow align with the expected charges • Ensure that the CHF system handles these multiple sessions and QoS flows accurately

1.Test No	GR_TSTP_3.12.2_A2
2. Test Details	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.
3. Test Instruments Required	Wireshark, UE + gNB simulator tool
4. Test Setup	Test Setup Small size 5G Core-1
5. Test Procedure	Action • Initiate Data Session with Multiple Service Flows • Simulate the initiation of a data session for a subscriber with multiple service data flows. • Verify FBC Charging for Service Flows • Validate that the CHF system accurately tracks data volumes for each service data flow associated with the session. Response: • Core has performed the initiated procedures
6. Test Limits	NA
7. Expected Results	• Ensure that each service data flow is associated with a unique rating group and service identifier. • Verify that the CHF system applies the tariff rates defined for each rating group and service identifier combination.

1.Test No	GR_TSTP_3.12.2_A3
2. Test Details	Integration of 4G Charging and 5G charging.
3. Test Instruments Required	Wireshark, UE + gNB simulator tool
4. Test Setup	Test Setup Small size 5G Core-1
5. Test Procedure	Action • Initiate Data Session in 4G Network • Simulate the initiation of a data session for a subscriber in a 4G network. • Verify Charging for 4G Network • Verify Charging for 5G Network • Validate that the CHF system calculates charges accurately for the 5G data session based on the configured tariff rates for 5G services. Response: • Core has performed the initiated procedures
6. Test Limits	NA
7. Expected Results	• Confirm that the CHF system identifies the network type as 4G and applies the corresponding tariff rates for charging. • Ensure that the calculated charges match the expected charges for the 5G session

1.Test No	GR_TSTP_3.12.2_A4
2. Test Details	Charging of services based on network slice, as well as charging as per network slice management
3. Test Instruments Required	Wireshark, UE + gNB simulator tool
4. Test Setup	Test Setup Small size 5G Core-1
5. Test Procedure	Action • Initiate Data Session within a Network Slice • Simulate the initiation of a data session for a subscriber within a specific network slice. • Verify Charging for Network Slice • Validate that the CHF system calculates charges accurately for the data session based on the charging parameters defined for the network slice. Response: • Core has performed the initiated procedures
6. Test Limits	NA
7. Expected Results	• Confirm that the CHF system identifies the network slice and applies the corresponding charging parameters. • Ensure that the calculated charges match the expected charges for the network slice session.

1.Test No	GR_TSTP_3.12.2_A5
2. Test Details	PDU session charging (data volumes are collected per user and per PDU session).
3. Test Instruments Required	Wireshark, UE + gNB simulator tool
4. Test Setup	Test Setup Small size 5G Core-1
5. Test Procedure	Action • Verify PDU Session Charging • Validate that the CHF system accurately tracks data volumes for the PDU session associated with the subscriber. • Validate Data Volume Collection • Confirm that the CHF system correctly collects data volumes for the entire duration of the PDU session. Response: • Core has performed the initiated procedures
6. Test Limits	NA
7. Expected Results	• Verify that the CHF system applies the tariff rates defined for PDU session charging. • Validate that the collected data volumes are accurately reflected in the charging calculations.

1.Test No	GR_TSTP_3.13_A
2. Test Details	The SMSF may support convergent charging towards CHF.
3. Test Instruments Required	Wireshark, UE + gNB simulator tool
4. Test Setup	Test Setup Small size 5G Core-1
5. Test Procedure	Action • Access the SMSF management interface using valid credentials. • Confirm that the SMSF processes the charging event without errors or exceptions. • Ensure that the charging amount and currency (CHF) are accurately calculated and processed. • Validate that the appropriate charging rules, discounts, and tariffs are applied as defined. • Check if the SMSF generates the expected charging records and notifications for the event. Response: • Core has performed the initiated procedures • The SMSF remains operational after the test and maintains its normal functionality.
6. Test Limits	NA
7. Expected Results	• The SMSF management interface is successfully accessed using valid credentials • Processes the charging event without errors. • Accurately calculates and processes the charging amount in CHF. • Applies the defined charging rules, discounts, and tariffs as expected. • Generates accurate charging records and notifications for the event

1.Test No	GR_TSTP_3.14_A1
2. Test Details	The NWDAF shall support one or more of the following functionalities: Identifier of network slice instance;
3. Test Instruments Required	Wireshark, UE + gNB simulator tool
4. Test Setup	Test Setup Small size 5G Core-1
5. Test Procedure	Action • Enter a valid network slice instance identifier into the designated field. • Initiate a request to retrieve information associated with the provided identifier. • Verify that the NWDAF responds with the relevant information related to the identified network slice instance. Response: • Core has performed the initiated procedures • The NF consumer application should be able to successfully subscribe to and unsub
6. Test Limits	NA
7. Expected Results	• The NWDAF provides accurate and relevant information associated with the provided network slice instance identifier.

1.Test No	GR_TSTP_3.14_A2
2. Test Details	load level information for that network slice instance
3. Test Instruments Required	Wireshark, UE + gNB simulator tool
4. Test Setup	Test Setup Small size 5G Core-1
5. Test Procedure	Action • Access the NWSAF functionality interface. • Verify that there is a dedicated functionality or API endpoint for retrieving load level information for a network slice instance. Response: • Core has performed the initiated procedures • The NF consumer application should be able to successfully subscribe to and unsubscribe from periodic and threshold exceeded notifications as intended.
6. Test Limits	NA
7. Expected Results	• The NWSAF interface includes a functionality or API endpoint related to retrieving load level information.

1.Test No	GR_TSTP_3.14_A3
2. Test Details	Support data collection from NFs and AFs;
3. Test Instruments Required	Wireshark, UE + gNB simulator tool
4. Test Setup	Test Setup Small size 5G Core-1
5. Test Procedure	Action • Access the NWSAF functionality interface. • Verify that there is a designated mechanism or API for initiating data collection from both NFs and Afs. • Identify a specific NF within the network environment. • Initiate a data collection request for the identified NF using the NWSAF interface. • Verify that the NWSAF receives the data from the NF, which may include performance metrics, status updates, or other relevant information Response: • Core has performed the initiated procedures • The NWSAF should demonstrate proper support for collecting accurate data from both NFs and AFs. • Collected data should be stored and processed correctly for further analysis and decision-making
6. Test Limits	NA
7. Expected Results	• The NWSAF interface includes a mechanism or API for data collection from both NFs and Afs. • The NWSAF successfully collects data from the NF and accurately processes and stores the received information.

1.Test No	GR_TSTP_3.14_A4
2. Test Details	Support data collection from OAM;
3. Test Instruments Required	Wireshark, UE + gNB simulator tool
4. Test Setup	Test Setup Small size 5G Core-1
5. Test Procedure	Action • Access the NWSAF functionality interface. • Verify that there is a dedicated mechanism or API for initiating data collection from the OAM system • Initiate a data collection request from the OAM system using the NWSAF interface. • Monitor the communication between the NWSAF and the OAM system to ensure the successful transfer of requested data. • Verify that the collected data from the OAM system includes relevant operational, administrative, or maintenance information. Response: • The NWSAF should demonstrate proper support for collecting accurate data from the OAM system. • Collected OAM data should be stored and processed correctly for further analysis and network management. • Core has performed the initiated procedures
6. Test Limits	NA
7. Expected Results	• The NWSAF interface includes a mechanism or API for data collection from the OAM system. • The NWSAF successfully collects data from the OAM system and accurately processes and stores the received information.

1.Test No	GR_TSTP_3.14_A5
2. Test Details	NWDAF service registration and metadata exposure to NFs and Afs
3. Test Instruments Required	Wireshark, UE + gNB simulator tool
4. Test Setup	Test Setup Small size 5G Core-1
5. Test Procedure	Action • Access the NWDAF service registration interface. • Verify that there is a mechanism or API for NFs and AFs to register their services with the NWDAF. • Access the NWDAF metadata exposure interface. • Verify that there is a mechanism or API for NFs and AFs to access metadata exposed by the NWDAF. Response: • Core has performed the initiated procedures • The NWDAF should demonstrate proper support for service registration by NFs and AFs, as well as accurate metadata exposure. • Exposed metadata should accurately reflect the behavior and performance of the registered services.
6. Test Limits	NA
7. Expected Results	• The NWDAF acknowledges the successful registration of the AF's service. • The NWDAF interface includes a mechanism or API for accessing metadata exposed to NFs and AFs.

1.Test No	GR_TSTP_3.14_A6
2. Test Details	Support analytics information provisioning to NFs and AFs
3. Test Instruments Required	Wireshark, UE + gNB simulator tool
4. Test Setup	Test Setup Small size 5G Core-1
5. Test Procedure	Action • Access the NWDAF analytics provisioning interface. • Verify that there is a mechanism or API for NFs and AFs to request and receive analytics information from the NWDAF. • Select a specific NF within the network environment. • Initiate a request for analytics information related to the selected NF's performance or behavior using the NWDAF interface. • Verify that the NWDAF provides accurate analytics information to the NF, which may include insights, trends, and recommendations Response: • Core has performed the initiated procedures • The NWDAF should demonstrate proper support for analytics information provisioning to NFs and AFs. • Analytics information should be accurate, insightful, and applicable for decision-making and optimization.
6. Test Limits	NA
7. Expected Results	• The NWDAF interface includes a mechanism or API for analytics information provisioning to NFs and Afs. • he NWDAF successfully provides accurate analytics information to the NF.

1.Test No	GR_TSTP_3.14_A7
2. Test Details	Support Machine Learning (ML) model training and provisioning to NWDAFs (containing Analytics logical function).
3. Test Instruments Required	Wireshark, UE + gNB simulator tool
4. Test Setup	Test Setup Small size 5G Core-1
5. Test Procedure	Action • Access the NWDAF interface with ML model training functionality. • Verify that there is a mechanism or API for initiating ML model training using historical data. • Repair historical data relevant to the specific network behavior or application performance. • Initiate ML model training request using the NWDAF interface, providing the prepared training dataset. • Monitor the training process to ensure it completes successfully without errors. Response: • Core has performed the initiated procedures • The NWDAF with Analytics logical function should demonstrate proper support for ML model training and provisioning. • Trained ML models should be successfully provisioned to NFs and AFs, enabling them to make data-driven predictions and decisions.
6. Test Limits	NA
7. Expected Results	• The NWDAF interface includes a mechanism or API for ML model training • he NWDAF should successfully train the ML model using the provided historical data.

1.Test No	GR_TSTP_3.14_B
2. Test Details	The NWDAF may allow NF consumers to subscribe to and unsubscribe from periodic notification and/or notification when a threshold is exceeded.
3. Test Instruments Required	Wireshark, UE + gNB simulator tool
4. Test Setup	Test Setup Small size 5G Core-1
5. Test Procedure	Action • Launch the NF consumer application, Access the NWDAF subscription interface. • Select the option to subscribe to periodic notifications. • Set the desired frequency of periodic notifications. • Confirm the subscription request. • Access the NWDAF subscription interface. • Select the option to unsubscribe from periodic notifications. • Confirm the un-subscription request. Response: • Core has performed the initiated procedures • The NF consumer application should be able to successfully subscribe to and unsubscribe from periodic and threshold exceeded notifications as intended.
6. Test Limits	NA
7. Expected Results	• The NF consumer application receives a subscription confirmation and starts receiving periodic notifications at the specified frequency. • The NF consumer application receives an un-subscription confirmation and stops receiving periodic notifications.

1.Test No	GR_TSTP_3.15_A1
2. Test Details	The Security Edge Protection Proxy (SEPP) is a non-transparent proxy and shall support: 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.
3. Test Instruments Required	• Wireshark, UE + gNB simulator tool • SEPP is deployed, configured, and operational. • Inter-PLMN control plane interfaces are properly established and functional. • Relevant security configurations and policies are correctly set up within SEPP.
4. Test Setup	Test Setup Small size 5G Core-1
5. Test Procedure	Action • Initiate a control plane message from PLMN-A to PLMN-B. • Monitor the transmission of the message and its reception by SEPP. • Verify that SEPP correctly filters incoming control plane messages. • Send control plane messages containing both allowed and disallowed attributes to SEPP. • Monitor SEPP's response and its handling of the disallowed attributes. • Send control plane messages that exceed predefined limits or violate established policies. • Monitor SEPP's response to the excessive or non-compliant messages. • Verify that SEPP enforces the appropriate policing actions, such as dropping or rate limiting. • Initiate a control plane message from PLMN-A to PLMN-B that adheres to established policies. • Monitor SEPP's processing of the authorized message. • Confirm that the authorized message is relayed to the intended destination. Response: • Core has performed the initiated procedures. • SEPP maintains the ability to filter, police, and enforce control plane message handling on inter-PLMN interfaces • Authorized and compliant control plane messages are relayed as intended.
6. Test Limits	NA
7. Expected Results	• Inter-PLMN communication is initiated, and the control plane message is transmitted and received by SEPP. • SEPP accurately filters incoming control plane messages based on allowed and disallowed attributes. • SEPP enforces policing actions on messages that exceed limits or violate established policies. • Control plane messages complying with policies are successfully processed and relayed by SEPP.

1.Test No	GR_TSTP_3.15_A2
2. Test Details	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.
3. Test Instruments Required	• Wireshark, UE + gNB simulator tool • SEPP is deployed, configured, and operational in both PLMN-A and PLMN-B. • Inter-PLMN control plane interfaces are properly established and operational. • Security configurations are set up between SEPPs and IPX entities. • Relevant Service Producer and Service Consumer entities are functional..
4. Test Setup	UE + gNB simulator tool, AMF, SMF, UPF, UDM, AUSF, UDR, NRF, PCF, NEF, NSSF, BSF
5. Test Procedure	Action • Initiate a service interaction request from the Service Producer in PLMN-A to the Service Consumer in PLMN-B. • Monitor the initiation of the service interaction and the message's path. • Verify that SEPP in PLMN-A correctly intercepts the service interaction message. • Confirm that SEPP applies topology hiding, masking the actual path and network details from Service Producer. • Monitor SEPP's relaying of the service interaction message to the SEPP in PLMN-B. • Ensure that SEPP in PLMN-B receives the relayed message and processes it for the Service Consumer. • Compare the result of the service interaction relayed by SEPPs to a direct interaction. • Confirm that the results are equivalent, indicating the successful service relaying by SEPPs. • Initiate a control plane message between SEPPs in PLMN-A and PLMNB. • Monitor the transmission of the message via IPX entities. Response: • Core has performed the initiated procedures. • Service interactions between Service Producer and Consumer are effectively relayed by SEPPs. • SEPPs maintain the ability to hide network topology, relay
6. Test Limits	NA

7. Expected Results	• Service interaction request from the Service Producer in PLMN-A is successfully initiated. • SEPP in PLMN-A applies topology hiding to the service interaction, masking network details. • SEPP in PLMN-B correctly relays the service interaction message for processing by the Service Consumer. • The results of the relayed service interaction are equivalent to a direct interaction. • Control plane messages between SEPPs pass successfully via IPX entities

1.Test No	GR_TSTP_3.15_A3
2. Test Details	The SEPP is a non-transparent proxy and shall support N32 interface
3. Test Instruments Required	• Wireshark, UE + gNB simulator tool • SEPP is deployed, configured, and operational in both PLMN-A and PLMN-B. • Inter-PLMN control plane interfaces are properly established and operational. • Security configurations are set up between SEPPs and IPX entities. • Relevant Service Producer and Service Consumer entities are functional.
4. Test Setup	UE + gNB simulator tool, AMF, SMF, UPF, UDM, AUSF, UDR, NRF, PCF, NEF, NSSF, BSF
5. Test Procedure	**Action:** • Initiate inter-PLMN communication (e.g., NF discovery, PDU session signaling) over **N32**. • SEPP intercepts and routes messages between V-PLMN and H-PLMN. • Verify SEPP enforces security policies (message integrity, authentication, and confidentiality). • Capture N32 signaling using Wireshark to observe SEPP behavior. **Response:** • SEPP forwards messages correctly between PLMNs without modifying payload (non-transparent proxy behavior). • Security functions (signing, encryption) applied as per 3GPP standards. • NFs in each PLMN successfully exchange messages over N32.
6. Test Limits	NA
7. Expected Results	• SEPP operates as a **non-transparent proxy** on the N32 interface. • Inter-PLMN signaling passes securely through SEPP. • Messages are routed correctly without loss or modification. • Wireshark traces confirm N32 communication and SEPP security processing per **3GPP TS 33.501**.

1.Test No	GR_TSTP_3.16_A
2. Test Details	SCP shall support Communication security (e.g., authorization of the NF Service Consumer to access the NF Service Producer API), load balancing, monitoring, overload control etc.
3. Test Instruments Required	Wireshark, UE + gNB simulator tool
4. Test Setup	UE + gNB simulator tool, AMF, SMF, UPF, UDM, AUSF, UDR, NRF, PCF, NEF, NSSF, BSF
5. Test Procedure	Action • Initiate a communication session between two entities through SCP • Initiate a secure communication session and monitor the key exchange process. • Attempt to intercept and analyze the exchanged keys. Response: • Between Nf-A and Nf-B SCP initiate procedure
6. Test Limits	NA
7. Expected Results	Exchanged keys should remain confidential and resistant to interception.

1.Test No	GR_TSTP_3.16_B
2. Test Details	The SCP includes one or more of the following functionalities: (I) Indirect Communication; (II) Delegated Discovery; (III) Message forwarding and routing to destination NF/NF service; and (IV) Message forwarding and routing to a next hop SCP
3. Test Instruments Required	Wireshark, UE + gNB simulator tool
4. Test Setup	UE + gNB simulator tool, AMF, SMF, UPF, UDM, AUSF, UDR, NRF, PCF, NEF, NSSF, BSF
5. Test Procedure	Action • Establish communication between two entities through SCP • Exchange test messages and data between the entities • Send encrypted data through SCP and ensure decryption at the destination. • Modify a packet in transit and verify that SCP detects the tampering • Attempt unauthorized access and confirm SCP denies it • Verify SCP enforces access control policies • Validate secure key exchange between entities through SCP Response: • Between Nf-A and Nf-B SCP initiate procedure
6. Test Limits	NA
7. Expected Results	• Entities can communicate seamlessly via the SCP. • SCP effectively ensures data confidentiality, integrity, authenticity, and access control. • SCP supports communication across various devices and services

1.Test No	GR_TSTP_3.16_C
2. Test Details	The SCP may support communication security (e.g. authorization of the NF Service Consumer to access the NF Service Producer API).
3. Test Instruments Required	Wireshark, UE + gNB simulator tool
4. Test Setup	UE + gNB simulator tool, AMF, SMF, UPF, UDM, AUSF, UDR, NRF, PCF, NEF, NSSF, BSF
5. Test Procedure	Action • Initiate a communication session between two entities through SCP • Initiate a secure communication session and monitor the key exchange process. • Attempt to intercept and analyze the exchanged keys. Response: • Between Nf-A and Nf-B SCP initiate procedure
6. Test Limits	NA
7. Expected Results	Exchanged keys should remain confidential and resistant to interception.

1.Test No	GR_TSTP_3.17_A1
2. Test Details	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.
3. Test Instruments Required	Wireshark, UE + gNB simulator tool N3IWF is deployed and operational UE is in an active state and capable of establishing an IKEv2/IPsec connection Necessary security configurations and keys are pre-established between N3IWF and 5G Core Network.
4. Test Setup	UE + gNB simulator tool, AMF, SMF, UPF, UDM, AUSF, UDR, NRF, PCF, NEF, NSSF, BSF
5. Test Procedure	Action • Initiate a connection request from the UE to the N3IWF. • Verify that N3IWF correctly negotiates IKEv2/IPsec parameters with the UE. • Confirm that IKE_SA (IKE Security Association) is successfully established • Validate that N3IWF extracts necessary authentication and authorization information from the IKEv2 exchange • Ensure that the 5G Core Network makes an authentication decision based on the relayed information. • Confirm that the UE's authorized services are determined based on the relayed session context. Response: • N3WIF Monitor the connection establishment process. • Core has performed the initiated procedures.
6. Test Limits	NA
7. Expected Results	• The connection between the UE and N3IWF is successfully initiated • N3IWF terminates the IKEv2/IPsec protocols with the UE and establishes IKE_SA • N3IWF accurately extracts, relays, and transmits authentication and authorization information to the 5G Core Network via N2 interface • The 5G Core Network receives the relayed information, authenticates the UE, and makes an authorization decision. • The UE is granted access to authorized services based on the relayed session context and security parameters.

1.Test No	GR_TSTP_3.17_A2
2. Test Details	Termination of N2 and N3 interfaces to 5G Core Network for control - plane and user-plane respectively.
3. Test Instruments Required	Wireshark, UE + gNB simulator tool N3IWF is deployed and operational 5G Core Network elements are operational and configured to communicate with N3IWF Required security configurations and keys are in place between N3IWF and the 5G Core Network.
4. Test Setup	UE + gNB simulator tool, AMF, SMF, UPF, UDM, AUSF, UDR, NRF, PCF, NEF, NSSF, BSF
5. Test Procedure	Action • Initiate a control-plane connection from the UE to the N3IWF. • Initiate a user-plane data transmission from the UE to the N3IWF. • Ensure that N3IWF correctly terminates the N2 control-plane interface • Confirm that the control-plane messages between the UE and the 5G Core Network are successfully relayed via N3IWF Response: • 3WIF Monitor the connection establishment process. • Core has performed the initiated procedures.
6. Test Limits	NA
7. Expected Results	• The control-plane connection between the UE and N3IWF is established successfully. • The user-plane data transmission between the UE and N3IWF is successful. • N3IWF accurately terminates the N2 control-plane interface and relays control-plane messages to the 5G Core Network. • N3IWF properly terminates the N3 user-plane interface and forwards data packets between the UE and the 5G Core Network

1.Test No	GR_TSTP_3.17_A3
2. Test Details	Relaying uplink and downlink control-plane NAS (N1) signaling between the UE and AMF.
3. Test Instruments Required	Wireshark, UE + gNB simulator tool N3IWF is deployed and operational Necessary security configurations and keys are established between N3IWF and the 5G Core Network.
4. Test Setup	UE + gNB simulator tool, AMF, SMF, UPF, UDM, AUSF, UDR, NRF, PCF, NEF, NSSF, BSF
5. Test Procedure	Action • Initiate an uplink and Downlink NAS signaling message from the UE to N3IWF • Verify that N3IWF correctly relays the uplink NAS message to AMF • Monitor the transmission and reception of the NAS message by AMF. Response: • 3WIF Monitor the connection establishment process. • Core has performed the initiated procedures.
6. Test Limits	NA
7. Expected Results	• Uplink and Downlink NAS signaling message from the UE is successfully transmitted and received by N3IWF. • N3IWF accurately relays the uplink and Downlink NAS message from the UE to AMF.

1.Test No	GR_TSTP_3.17_A4
2. Test Details	Handling of N2 signaling from SMF (relayed by AMF) related to PDU Sessions and QoS.
3. Test Instruments Required	Wireshark, UE + gNB simulator tool N3IWF is deployed and operational 5G Core Network elements, including AMF and SMF, are operational and configured. Necessary security configurations and keys are established between N3IWF and the 5G Core Network.
4. Test Setup	UE + gNB simulator tool, AMF, SMF, UPF, UDM, AUSF, UDR, NRF, PCF, NEF, NSSF, BSF
5. Test Procedure	Action • Initiate a PDU Session establishment request from the UE to N3IWF. • Verify that the SMF relays the PDU Session establishment request to AMF • Verify that N3IWF correctly processes the N2 signaling message related to PDU Session establishment. • Ensure N3IWF extracts the QoS parameters and other relevant information from the message. Response: • 3WIF Monitor the connection establishment process. • Core has performed the initiated procedures.
6. Test Limits	NA
7. Expected Results	• PDU Session establishment request from the UE is successfully transmitted and received by N3IWF. • N2 signaling message related to PDU Session establishment is successfully relayed by AMF and received by N3IWF. • N3IWF accurately processes the N2 signaling message, extracts QoS parameters, and prepares a response

1.Test No	GR_TSTP_3.17_A5
2. Test Details	Establishment of IPsec Security Association (IPsec SA) to support PDU Session traffic.
3. Test Instruments Required	Wireshark, UE + gNB simulator tool N3IWF is deployed and operational IPsec configuration, keys, and security policies are correctly set up between N3IWF and the 5G Core Network elements.
4. Test Setup	UE + gNB simulator tool, AMF, SMF, UPF, UDM, AUSF, UDR, NRF, PCF, NEF, NSSF, BSF
5. Test Procedure	Action • Initiate a PDU Session establishment request from the UE to N3IWF. • Verify that N3IWF correctly processes the PDU Session establishment request • Check that N3IWF establishes the necessary IPsec SA parameters based on the configured security policies. • Initiate data transmission (e.g., internet browsing) from the UE through the established PDU Session. • Monitor the data traffic as it passes through the IPsec SA. Response: • 3WIF Monitor the connection establishment process. • Core has performed the initiated procedures.
6. Test Limits	NA
7. Expected Results	• PDU Session establishment request from the UE is successfully transmitted and received by N3IWF. • N3IWF establishes the IPsec SA parameters required to secure the PDU Session traffic. • Secure PDU Session traffic flows through the established IPsec SA, maintaining confidentiality and integrity.

1.Test No	GR_TSTP_3.17_A6
2. Test Details	Relaying uplink and downlink user-plane packets between the UE and UPF. This involves: (I) De-capsulation/ encapsulation of packets for IPSec and N3 tunnelling; (II) 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; (III) Local mobility anchor within untrusted non-3GPP access networks using MOBIKE per IETF RFC 4555;
3. Test Instruments Required	• Wireshark, UE + gNB simulator tool • N3IWF is properly deployed, configured, and operational. • Untrusted non-3GPP access network is available • Appropriate security configurations, keys, and policies are established for IPSec and N3 tunneling • MOBIKE per IETF RFC 4555 is supported. • Multiple AMFs are available and configured • QoS policies are defined and supported.
4. Test Setup	UE + gNB simulator tool, AMF, SMF, UPF, UDM, AUSF, UDR, NRF, PCF, NEF, NSSF, BSF
5. Test Procedure	Action • Initiate uplink user-plane data transmission from the UE within the untrusted non-3GPP access network. • Verify that N3IWF correctly de-capsulates the user-plane packets received from the UE • Check that N3IWF encapsulates the packets for IPSec and N3 tunneling towards the UPF. • Monitor the encapsulation process and ensure the packets are ready for transmission. • Verify that N3IWF inspects the N3 packet marking to determine QoS requirements. • Confirm that N3IWF enforces the appropriate QoS policies based on packet marking. • Monitor the user-plane data transmission with enforced QoS. • Initiate a handover scenario within the untrusted non-3GPP access network. • Ensure MOBIKE support allows N3IWF to maintain communication during the handover. • Verify that N3IWF adjusts its connections as necessary to ensure continuity. • Verify that N3IWF selects the appropriate AMF based on the UE's location and operational requirements. Response: • 3WIF Monitor the connection establishment process. • Core has performed the initiated procedures.
6. Test Limits	NA
7. Expected Results	• Uplink user-plane data transmission from the UE is successfully relayed by

	N3IWF. • N3IWF correctly performs de-capsulation and encapsulation for IPSec and N3 tunneling. • QoS policies are enforced by N3IWF based on N3 packet marking. • MOBIKE support enables N3IWF to handle handover scenarios within the untrusted non-3GPP access network. • N3IWF selects the appropriate AMF and establishes the necessary connections.

1.Test No	GR_TSTP_3.18_A1
2. Test Details	To verify that the LMF determines the result of UE positioning in geographical coordinates as defined in TS 23.032 and, if requested and available, includes the velocity of the UE
3. Test Instruments Required	Wireshark, UE + gNB simulator tool
4. Test Setup	Test Setup Small size 5G Core-1
5. Test Procedure	**Action** • Configure LMF and establish connectivity with AMF and gNB. • Initiate a positioning request for a selected UE through LMF. • Ensure UE provides GNSS-based measurements to gNB and LMF. • Collect geographical coordinates computed by LMF based on received data. • Repeat test with velocity request enabled in the positioning query. **Response** • LMF calculates UE position in latitude, longitude, and altitude format. • Velocity information is included in the result when requested and available. • Positioning results are logged and displayed accurately.
6. Test Limits	NA
7. Expected Results	LMF successfully determines UE position in standard geographical coordinates and provides velocity data when requested.

1.Test No	GR_TSTP_3.18_B1
2. Test Details	The LMF may support Request for a single location received from a serving AMF for a target UE.
3. Test Instruments Required	Wireshark, UE + gNB Simulator Tool, LMF/AMF Emulator
4. Test Setup	UE + gNB simulator tool, AMF, SMF, UPF, UDM, AUSF, UDR, NRF, PCF, NEF, NSSF, BSF
5. Test Procedure	**Action:** • AMF sends a **single location request** to LMF for a target UE. • LMF collects measurements from UE and RAN. • LMF calculates UE location. • LMF responds to AMF with location result. • Capture signaling over N11 and user plane measurements using Wireshark. **Response:** • LMF successfully receives the request and computes UE location. • AMF receives accurate location information. • Signaling follows 3GPP procedures.
6. Test Limits	NA
7. Expected Results	• LMF correctly supports **single location requests** from AMF. • UE location is accurately computed and returned. • N11 signaling traces confirm correct **AMF ↔ LMF** interactions per **3GPP TS 23.273/38.455**. • Location response meets expected accuracy and timing requirements.

1.Test No	GR_TSTP_3.18_B2
2. Test Details	Request for periodic or triggered location received from a serving AMF for a target UE.
3. Test Instruments Required	Wireshark, UE + gNB Simulator Tool, LMF/AMF Emulator
4. Test Setup	UE + gNB simulator tool, AMF, SMF, UPF, UDM, AUSF, UDR, NRF, PCF, NEF, NSSF, BSF
5. Test Procedure	**Action:** • AMF sends a periodic or triggered location request to LMF for a target UE. • LMF collects measurements from UE and RAN periodically or on event triggers. • LMF calculates UE location at each interval or trigger. • LMF responds to AMF with location updates. • Capture signaling over N11 and user plane measurements using Wireshark. **Response:** • LMF successfully receives and processes periodic/triggered requests. • AMF receives continuous location updates for the UE. • Signaling follows 3GPP procedures for periodic and event-triggered reporting.
6. Test Limits	NA
7. Expected Results	• LMF correctly supports **periodic and triggered location requests** from AMF. • UE location is updated and returned accurately based on configured intervals or triggers. • N11 signaling traces confirm proper **AMF ↔ LMF** interactions per **3GPP TS 23.273/38.455**. • Location updates meet expected accuracy and timing requirements.

1.Test No	GR_TSTP_3.18_B3
2. Test Details	Determination of position methods based on UE and PLMN capabilities, QoS, UE connectivity state per access type and LCS Client type.
3. Test Instruments Required	Wireshark, UE + gNB Simulator Tool, LMF/AMF Emulator
4. Test Setup	UE + gNB simulator tool, AMF, SMF, UPF, UDM, AUSF, UDR, NRF, PCF, NEF, NSSF, BSF
5. Test Procedure	**Action:** • AMF forwards location request from LCS client to LMF for a target UE. • LMF evaluates UE capabilities, PLMN capabilities, QoS, UE connectivity state, and LCS client type. • LMF selects the most appropriate positioning method. • LMF requests measurements from UE and RAN as per selected method. • Capture signaling and positioning method selection process using Wireshark. **Response:** • LMF determines a suitable positioning method according to all inputs. • UE and network respond with measurements as required by the selected method. • Location results provided to AMF and LCS client per request type.
6. Test Limits	NA
7. Expected Results	• LMF correctly selects **positioning method** based on UE/PLMN capabilities, QoS, connectivity state, and LCS client type. • Location measurements follow selected method, and accurate results are returned. • N11 signaling traces confirm proper **AMF ↔ LMF** interaction and positioning method determination per **3GPP TS 23.271/23.273/38.455**. • Location accuracy meets expected requirements for requested QoS and client type.

1.Test No	GR_TSTP_3.18_B4
2. Test Details	Report of UE location estimates directly to a GMLC for periodic or triggered location of a target UE.
3. Test Instruments Required	Wireshark, UE + gNB Simulator Tool, LMF/AMF Emulator
4. Test Setup	UE + gNB simulator tool, AMF, SMF, UPF, UDM, AUSF, UDR, NRF, PCF, NEF, NSSF, BSF
5. Test Procedure	**Action:** • LCS client requests UE location via GMLC (periodic or triggered). • GMLC forwards request to LMF via AMF if required. • LMF collects measurements from UE and RAN. • LMF calculates UE location and reports estimates directly to GMLC. • Capture signaling over N11 and LCS interface using Wireshark. **Response:** • LMF successfully computes and sends UE location estimates to GMLC. • GMLC receives periodic or event-triggered updates as requested. • Signaling follows 3GPP procedures for location reporting.
6. Test Limits	NA
7. Expected Results	• LMF correctly reports **UE location estimates** to GMLC for both periodic and triggered requests. • Location updates are accurate and timely. • Signaling traces confirm proper **LMF ↔ GMLC** interaction per **3GPP TS 23.271/23.273/29.171**. • LCS client receives location information according to requested intervals or triggers.

1.Test No	GR_TSTP_3.18_B5
2. Test Details	Cancelation of periodic or triggered location for a target UE.
3. Test Instruments Required	Wireshark, UE + gNB Simulator Tool, LMF/AMF Emulator
4. Test Setup	UE + gNB simulator tool, AMF, SMF, UPF, UDM, AUSF, UDR, NRF, PCF, NEF, NSSF, BSF
5. Test Procedure	**Action:** • LCS client sends **cancellation request** for periodic or triggered location reporting via GMLC or AMF. • AMF forwards cancellation request to LMF. • LMF stops sending location updates for the target UE. • Capture signaling over N11 and LCS interface using Wireshark. **Response:** • LMF successfully cancels periodic or triggered location reporting. • No further location updates are sent to AMF or GMLC. • Signaling confirms that the cancellation request is acknowledged.
6. Test Limits	NA
7. Expected Results	• LMF correctly processes cancellation of periodic or triggered location requests. • UE location reporting stops immediately after cancellation. • N11 and LCS interface signaling traces confirm proper AMF ↔ LMF ↔ GMLC interactions per 3GPP TS 23.271/23.273/38.455. • System resources associated with the cancelled reporting are released appropriately.

1.Test No	GR_TSTP_3.18_B6
2. Test Details	Provision of broadcast assistance data to UEs via NG RAN in ciphered or unciphered form and forward any ciphering keys to subscribed UEs via the AMF.
3. Test Instruments Required	Wireshark, UE + gNB Simulator Tool, LMF/AMF Emulator
4. Test Setup	UE + gNB simulator tool, AMF, SMF, UPF, UDM, AUSF, UDR, NRF, PCF, NEF, NSSF, BSF
5. Test Procedure	**Action:** • Broadcast assistance data is prepared for transmission via NG-RAN. • For ciphered data, AMF forwards ciphering keys to subscribed UEs. • NG-RAN broadcasts assistance data to UEs. • UEs receive and, if applicable, decrypt data using keys from AMF. • Capture signaling and data delivery using Wireshark. **Response:** • UEs successfully receive broadcast assistance data. • Ciphered data is correctly decrypted using keys from AMF. • Signaling confirms secure key delivery and data broadcast.
6. Test Limits	NA
7. Expected Results	• Broadcast assistance data is correctly delivered to UEs in both **ciphered and unciphered forms**. • Ciphering keys are securely forwarded via AMF and used by UEs to decrypt data. • NG-RAN and AMF signaling traces confirm compliance with **3GPP TS 38.331/38.455/23.501**. • UEs receive accurate and timely broadcast assistance data without errors.

1.Test No	GR_TSTP_3.18_B7
2. Test Details	Change of a serving LMF for periodic or triggered location reporting for a target UE.
3. Test Instruments Required	Wireshark, UE + gNB Simulator Tool, LMF/AMF Emulator
4. Test Setup	UE + gNB simulator tool, AMF, SMF, UPF, UDM, AUSF, UDR, NRF, PCF, NEF, NSSF, BSF
5. Test Procedure	**Action:** • UE moves or conditions trigger the need for a **change of serving LMF**. • AMF coordinates the transfer from current LMF to target LMF. • Target LMF continues periodic or triggered location reporting to AMF/GMLC. • Capture signaling over N11 and LCS interface using Wireshark. **Response:** • Current LMF stops location reporting for the UE. • Target LMF receives required UE context and resumes periodic/triggered reporting. • AMF continues receiving seamless location updates. • Signaling confirms successful handover of serving LMF responsibilities.
6. Test Limits	NA
7. Expected Results	• Serving LMF is successfully changed without loss of location updates. • Periodic or triggered location reporting continues seamlessly after LMF change. • N11 and LCS interface traces confirm proper **AMF ↔ LMF** interactions per **3GPP TS 23.271/23.273/38.455**. • UE location accuracy and update intervals are maintained post-transfer.

1.Test No	GR_TSTP_3.19_A1
2. Test Details	Verify the CBCF shall be responsible for the management of CBS (Cell Broadcast Service) messages
3. Test Instruments Required	Wireshark, UE + gNB simulator tool
4. Test Setup	Test Setup Small size 5G Core-1
5. Test Procedure	**Action** • Configure CBCF and register it with the NRF. • Establish N32 interface between CBCF and AMF. • Create a CBS message in CBCF with message ID, serial number, data coding scheme, and target area. • Initiate CBS message distribution process from CBCF. **Response** • CBCF successfully registers and exchanges service discovery messages with NRF. • CBCF–AMF connectivity is verified. • CBCF accepts and stores the CBS message in its internal database with "Created" status. • CBCF initiates message broadcast procedure and updates lifecycle status ("Active", "Completed", or "Cancelled").
6. Test Limits	NA
7. Expected Results	CBCF successfully manages the CBS message creation, storage, and distribution. The message lifecycle is accurately maintained and logged in CBCF. AMF confirms receipt of broadcast instruction

1.Test No	GR_TSTP_3.19_A2
2. Test Details	To verify the Allocation of serial numbers
3. Test Instruments Required	Wireshark, UE + gNB simulator tool
4. Test Setup	Test Setup Small size 5G Core-1
5. Test Procedure	**Action** • Configure and register CBCF with the NRF. • Establish N32 interface between CBCF and AMF. • Create multiple CBS messages in CBCF for broadcast testing. • Observe serial number allocation for each created message. **Response** • CBCF successfully registers with NRF and communicates with AMF. • CBCF automatically allocates unique serial numbers for each CBS message. • Serial numbers are sequential, non-repetitive, and formatted according to 3GPP TS 23.041. • CBCF maintains a serial number table or log for tracking purposes.
6. Test Limits	NA
7. Expected Results	CBCF allocates unique and valid serial numbers for every CBS message created, ensuring correct message identification and traceability.

1.Test No	GR_TSTP_3.19_A3
2. Test Details	To verify Modifying or deleting CBS messages held by the NG-RAN node.
3. Test Instruments Required	Wireshark, UE + gNB simulator tool
4. Test Setup	Test Setup Small size 5G Core-1
5. Test Procedure	**Action** • Configure CBCF and establish connections with AMF and NG-RAN. • Create and distribute a CBS message from CBCF to the NG-RAN node. • After confirmation of message delivery, send a “Modify CBS Message” request from CBCF. • Then issue a “Delete CBS Message” command from CBCF to NG-RAN. **Response** • NG-RAN acknowledges receipt of the original CBS message. • Upon modify command, NG-RAN updates the message content or parameters as instructed by CBCF. • Upon delete command, NG-RAN removes the message from its active broadcast list and confirms deletion. • CBCF updates internal logs showing successful modification and deletion transactions.
6. Test Limits	NA
7. Expected Results	CBCF successfully modifies or deletes CBS messages stored in NG-RAN nodes. NG-RAN confirms each operation, and CBCF records corresponding message status updates.

1.Test No	GR_TSTP_3.19_A4
2. Test Details	To Verify Initiating broadcast by sending fixed-length CBS messages to an NG-RAN node for each language provided by the cell, and where necessary padding the pages to a length of 82 octets (see 3GPP TS 23.038 [3]).
3. Test Instruments Required	Wireshark, UE + gNB simulator tool
4. Test Setup	Test Setup Small size 5G Core-1
5. Test Procedure	**Action** • Configure CBCF and ensure NG-RAN connection is active. • Create multilingual CBS messages in CBCF (e.g., English, Hindi, Tamil). • Ensure each message payload conforms to fixed 82-octet length; pad where required. • Initiate broadcast from CBCF to NG-RAN for all language variants. **Response** • NG-RAN receives and acknowledges each language-specific CBS message.
6. Test Limits	NA
7. Expected Results	CBCF initiates broadcast of fixed-length CBS messages for each supported language, with correct padding applied. NG-RAN confirms successful receipt of all messages.

1.Test No	GR_TSTP_3.19_A5
2. Test Details	To verify Determining the set of cells to which a CBS message should be broadcast, and indicating within the Serial Number the geographical scope of each CBS message
3. Test Instruments Required	Wireshark, UE + gNB simulator tool
4. Test Setup	Test Setup Small size 5G Core-1
5. Test Procedure	**Action** • Configure CBCF with predefined cell and TA (Tracking Area) mapping. • Create a CBS message and select broadcast coverage criteria (e.g., TA1, TA2). • Initiate broadcast request from CBCF toward NG-RAN, ensuring the serial number encodes the geographical scope. **Response** • CBCF identifies correct set of cells matching the specified broadcast area. • CBCF embeds appropriate geographical scope information in the message serial number. • NG-RAN acknowledges receipt and prepares broadcast for the selected cells.
6. Test Limits	NA
7. Expected Results	CBCF correctly determines the target cells and encodes the geographical scope in the serial number. NG-RAN confirms correct area-based message delivery.

1.Test No	GR_TSTP_3.19_A6
2. Test Details	To verify that the CBCF determines the time at which a CBS message should commence being broadcast.
3. Test Instruments Required	Wireshark, UE + gNB simulator tool
4. Test Setup	Test Setup Small size 5G Core-1
5. Test Procedure	**Action** • Configure CBCF and establish connectivity with NG-RAN. • Create a CBS message and set a defined broadcast start time (e.g., 10:00:00). • Initiate the broadcast scheduling request from CBCF. **Response** • CBCF saves and schedules the broadcast request with the defined start time. • CBCF triggers message transmission exactly at the scheduled time. • NG-RAN begins the broadcast according to the defined time window.
6. Test Limits	NA
7. Expected Results	CBCF correctly determines and enforces the broadcast start time. NG-RAN initiates message transmission within the allowed time tolerance.

1.Test No	GR_TSTP_3.19_A7
2. Test Details	To verify that the CBCF determines the time at which a CBS message should cease being broadcast and instructs each NG-RAN node to stop the broadcast.
3. Test Instruments Required	Wireshark, UE + gNB simulator tool
4. Test Setup	Test Setup Small size 5G Core-1
5. Test Procedure	**Action** • Configure CBCF and establish connectivity with NG-RAN. • Create a CBS message with defined start and stop times. • Initiate message broadcast and allow it to run until stop time. • Observe CBCF behavior at broadcast end time. **Response** • CBCF monitors broadcast duration and triggers stop command at end time. • NG-RAN acknowledges receipt of stop instruction. • CBCF logs completion and marks message as "Ceased."
6. Test Limits	NA
7. Expected Results	CBCF terminates CBS message broadcast at the defined stop time and receives confirmation from NG-RAN that transmission has ceased.

1.Test No	GR_TSTP_3.19_A8
2. Test Details	To verify that the CBCF determines the period at which broadcast of the CBS message should be repeated.
3. Test Instruments Required	Wireshark, UE + gNB simulator tool
4. Test Setup	Test Setup Small size 5G Core-1
5. Test Procedure	**Action** • Configure CBCF and establish connection with NG-RAN. • Create a CBS message and define a repetition interval (e.g., every 5 minutes). • Initiate broadcast scheduling request including repetition setting. • Observe CBCF over multiple broadcast cycles. **Response** • CBCF schedules message re-broadcast at defined intervals. • NG-RAN receives and performs each broadcast repetition. • CBCF logs broadcast events for each repetition period.
6. Test Limits	NA
7. Expected Results	CBCF correctly determines and enforces the broadcast repetition period, ensuring consistent message retransmission by NG-RAN.

1.Test No	GR_TSTP_3.19_A9
2. Test Details	To verify that the CBCF allocates an "emergency indication" to CBS messages when transmitting emergency alerts, differentiating them from normal CBS messages.
3. Test Instruments Required	Wireshark, UE + gNB simulator tool
4. Test Setup	Test Setup Small size 5G Core-1
5. Test Procedure	**Action** • Configure CBCF and confirm NG-RAN connectivity. • Create a normal CBS message and an emergency CBS message. • Assign "emergency indication" parameter to the emergency message. • Initiate broadcast of both message types sequentially. **Response** • CBCF marks emergency message with emergency flag. • NG-RAN identifies and processes the message as an emergency alert. • CBCF logs confirmation of emergency indication assignment.
6. Test Limits	NA
7. Expected Results	CBCF correctly allocates the "emergency indication" to emergency CBS messages, ensuring they are distinguished from standard broadcasts and handled with priority.

1.Test No	GR_TSTP_4
2. Test Details	To verify that the IP Multimedia Subsystem (IMS) provides the following functionalities within the Small Size 5G Core System: (I) IMS functionality for supporting SMS. (II) IMS functionality for Voice and Video Service over 5G Network. (III) SIP & RTP interface for external interface towards IP PABX/MGW for voice interworking.
3. Test Instruments Required	Wireshark, UE + gNB simulator tool SIP/RTP analyzer P PABX/MGW simulator
4. Test Setup	Test Setup Small size 5G Core-1
5. Test Procedure	**Action** • Configure IMS core components (P-CSCF, I-CSCF, S-CSCF, HSS). • Integrate IMS with AMF and SMF using N5/N33 interfaces. • Register multiple UEs via SIP REGISTER through IMS. • Initiate SMS delivery over IMS using SIP MESSAGE. • Establish SIP INVITE sessions for both voice and video calls between UEs. • Verify RTP media flow for both services. • Configure and validate SIP/RTP interworking with external IP PABX/MGW for voice. **Response** • IMS successfully registers UEs and manages SIP sessions for SMS, voice, and video. • RTP paths establish correctly for both call types. • IP PABX/MGW confirms SIP/RTP interworking for external calls.
6. Test Limits	NA
7. Expected Results	IMS core supports SMS, voice, and video services over 5G using SIP/RTP protocols, ensuring proper session control and interworking with IP PABX/MGW.

1.Test No	GR_TSTP_5.1_A
2. Test Details	Verification of Configuration changes related to 5G core/User related
3. Test Instruments Required	Wireshark, UE + gNB simulator tool, NMS (Network Management System) Testing Environment
4. Test Setup	Test Setup Small size 5G Core-2
5. Test Procedure	Action: • apply Configuration change in given configuration files and verify Configuration changes Response: • Configuration changes applied successfully
6. Test Limits	NA
7. Expected Results	• Configuration changes should be reflected correctly

1.Test No	GR_TSTP_5.1_B
2. Test Details	Verification of alarm and Fault reporting in 5G core
3. Test Instruments Required	Wireshark, UE + gNB simulator tool, NMS (Network Management System) Testing Environment
4. Test Setup	Test Setup Small size 5G Core-2
5. Test Procedure	Action: Ng-Interface down, alarm Reported by NMS Response: Verify that the NMS accurately identifies, reports, any Alarm Related to event
6. Test Limits	NA
7. Expected Results	• Successful identification and reporting of faults and alarms by the NMS.

1.Test No	GR_TSTP_5.1_C
2. Test Details	Verification of Performance KPI through NMS
3. Test Instruments Required	Wireshark, UE + gNB simulator tool, NMS (Network Management System) Testing Environment
4. Test Setup	Test Setup Small size 5G Core-2
5. Test Procedure	Action: perform multiple UE registration, PDU session establishment. Response: verification of Performance KPI like – Number of Registration, deregistration and types of Registration, Number of established PDU session per NF
6. Test Limits	NA
7. Expected Results	• Performance KPI should be reflected per NF

1.Test No	GR_TSTP_5.1_D
2. Test Details	Verification of NMS's capability to handle storage for both system software and data.
3. Test Instruments Required	Wireshark, UE + gNB simulator tool, NMS (Network Management System) Testing Environment
4. Test Setup	Test Setup Small size 5G Core-2
5. Test Procedure	Action: perform storage of configuration files perform restore of backup file Response: File storage successful Restoration of backup file successful
6. Test Limits	NA
7. Expected Results	successfully stored configuration files • successfully restore backup of configuration files

1.Test No	GR_TSTP_5.1_E
2.Test Details	Verification of security feature enabled in NMS
3. Test Instruments Required	Wireshark, UE + gNB simulator tool, NMS (Network Management System) Testing Environment
4. Test Setup	Test Setup Small size 5G Core-2
5. Test Procedure	Action: Tried to Attempt login with unauthorized credential Response: Verify that NMS prevent unauthorized access and provide message as credential are invalid.
6. Test Limits	NA
7. Expected Results	NMS should reply with message as invalid credential

1.Test No	GR_TSTP_5.2_A
2. Test Details	To verify that the OMC utilizes a relational or object-oriented database to store and manage necessary parameter information as per system requirements.
3. Test Instruments Required	Wireshark, UE + gNB simulator tool, OMC
4. Test Setup	Test Setup Small size 5G Core-2
5. Test Procedure	Action: • Perform Storage activity to store Related Configuration and performance related data. Response: • successfully able to store related configuration • successfully able to store performance data
6. Test Limits	NA
7. Expected Results	Related configuration storage successful • Related performance data storage successful

1.Test No	GR_TSTP_5.2_B
2. Test Details	To verify that the OMC database includes configuration data, maintenance data, fault data, and performance/QoS data as per system requirements.
3. Test Instruments Required	Wireshark, UE + gNB simulator tool, OMC
4. Test Setup	Test Setup Small size 5G Core-2
5. Test Procedure	Action: • Perform activity to include Configuration data • Perform activity to include Maintenance/Fault data • Perform activity to include Performance data Response: • successfully able to reflect configuration, Maintenance and Performance data
6. Test Limits	NA
7. Expected Results	OMC database should store and reflect configuration, Maintenance and Performance Related data.

1.Test No	GR_TSTP_5.2_C
2. Test Details	TTo verify that the OMC database resides on a disk with mirroring capability to ensure data redundancy and reliability.
3. Test Instruments Required	Wireshark, UE + gNB simulator tool, OMC
4. Test Setup	Test Setup Small size 5G Core-2
5. Test Procedure	Action: • Perform Activity to store configuration data in database Response: • OMC able to mirror store data in backup disk in real time
6. Test Limits	NA
7. Expected Results	A Separate Disk volume created by OMC in physical disk to store configuration/performance data

1.Test No	GR_TSTP_5.2_D
2. Test Details	To verify that the OMC is capable of storing generated performance data, with clearly defined storage methods and capacity as per system specifications.
3. Test Instruments Required	Wireshark, UE + gNB simulator tool, OMC
4. Test Setup	Test Setup Small size 5G Core-2
5. Test Procedure	Action: • Perform Activity to store performance related data in database Response: • OMC able to store performance data and reflect storage capacity
6. Test Limits	NA
7. Expected Results	Able to Store generated performance data and reflect storage capacity

1.Test No	GR_TSTP_5.2_E
2. Test Details	To verify that the OMC provides configurable provisions for collecting statistical information related to network events at a defined frequency.
3. Test Instruments Required	Wireshark, UE + gNB simulator tool, OMC
4. Test Setup	Test Setup Small size 5G Core-2
5. Test Procedure	Action: • Perform Activity to store performance related data with daily/hourly and weekly Response: • OMC able to store performance data on with daily/hourly and weekly
6. Test Limits	NA
7. Expected Results	Able to Store generated performance data on frequency basis

1.Test No	GR_TSTP_5.2_F
2. Test Details	To verify that the OMC database maintains the fault history of the entire network and supports searching and displaying data based on Network Elements, Severity Class, and Event Type.
3. Test Instruments Required	Wireshark, UE + gNB simulator tool, OMC
4. Test Setup	Test Setup Small size 5G Core-2
5. Test Procedure	Action: • perform fault history based on 5G network element • perform fault history based on severity class Critical/Major/Minor • perform fault history based on Event and its type Response: • able to search fault history based on selected Network element • able to search fault history based on severity class Critical/Major/Minor • able to search fault history based on Event and its type
6. Test Limits	NA
7. Expected Results	OMC display all fault history based on history monthly/weekly basis for selected Network Element OMC display all fault history based on severity class Critical/Major/Minor OMC display all fault history based on Event and its type

1.Test No	GR_TSTP_5.3_A
2. Test Details	Assesses the OMC (Operations and Maintenance Center) software's compatibility
3. Test Instruments Required	Wireshark, UE + gNB simulator tool, OMC
4. Test Setup	Test Setup Small size 5G Core-2
5. Test Procedure	Action: • Install and configure OMC software on UNIX, LINUX, and Windows platforms. Response: • Confirm successful installation and configuration on all tested platforms.
6. Test Limits	NA
7. Expected Results	Able to install OMC software on different software platform successfully.

1.Test No	GR_TSTP_5.3_B
2.Test Details	Verification of support of interface with NMS like like CORBA / TCP / IP / CMIP / SNMP/ REST / HTTP to enable it to work with a remote NMS.
3. Test Instruments Required	Wireshark, UE + gNB simulator tool, OMC, Interfaces
4. Test Setup	Test Setup Small size 5G Core-2
5. Test Procedure	Action: • Perform Remote working with NMS using interface of HTTP Response: • Successfully able to Login NMS using HTTP interface
6. Test Limits	NA
7. Expected Results	Should be able to remotely logging using HTTP interface remotely

1.Test No	GR_TSTP_5.3_D
2. Test Details	Verification of support Ethernet connectivity with NMS and Network element
3. Test Instruments Required	Wireshark, UE + gNB simulator tool, OMC, Ethernet Interface
4. Test Setup	Test Setup Small size 5G Core-2
5. Test Procedure	Action: • perform Ethernet connectivity with remote network elements via LAN cable. Response: • Successfully able to Login NMS using Ethernet Interface
6. Test Limits	NA
7. Expected Results	Should be able to remotely logging using Ethernet interface

1.Test No	GR_TSTP_5.3_E
2. Test Details	To verify that the OMC provides a Graphical User Interface (GUI) or management through an Element Management System (EMS) for efficient network monitoring and control.
3. Test Instruments Required	Wireshark, UE + gNB simulator tool, OMC
4. Test Setup	Test Setup Small size 5G Core-2
5. Test Procedure	Action: • perform operation with OMC GUI Response: • Successfully able to Login and perform Action with OMC GUI
6. Test Limits	NA
7. Expected Results	Should be able to login and perform action using OMC GUI

1.Test No	GR_TSTP_5.3_F
2. Test Details	To verify that the OMC provides an on-line help feature for user assistance and guidance.
3. Test Instruments Required	Wireshark, UE + gNB simulator tool, OMC
4. Test Setup	Test Setup Small size 5G Core-2
5. Test Procedure	Action: • perform On line help option to contact concerned team Response: • Successfully able to Login and perform Action with OMC GUI
6. Test Limits	NA
7. Expected Results	Should be able to login and perform action using OMC GUI

1.Test No	GR_TSTP_5.3_G
2. Test Details	To verify that the OMC ensures data consistency, monitors alarm status, maintains event logs, and collects performance counters as per system requirements.
3. Test Instruments Required	Wireshark, UE + gNB simulator tool, OMC
4. Test Setup	Test Setup Small size 5G Core-2
5. Test Procedure	Action: • Perform data consistency check using pre-defined template • Perform alarm status check based on class Response: • Successfully able check and verify data consistency • Successfully able to check alarm status
6. Test Limits	NA
7. Expected Results	Should be able to perform action to check Alarm Status/consistency check / performance counter

1.Test No	GR_TSTP_5.3_K
2. Test Details	To verify that the OMC enforces limited access based on user classification (Admin User/Public User) to ensure role-based security and control.
3. Test Instruments Required	Wireshark, UE + gNB simulator tool, OMC
4. Test Setup	Test Setup Small size 5G Core-2
5. Test Procedure	Action: • Perform All kind of Action in OMC with Admin user • Perform All kind of Action in OMC with Public user Response: • Limited access with public user account which is not exposed to all common user
6. Test Limits	NA
7. Expected Results	• Admin related access Restricted and not be entertained by public user account

1.Test No	GR_TSTP_6.1_A
2. Test Details	To verify that the OMC provides a flexible and secure management interface for configuration, performance, and fault management, including debugging and troubleshooting.
3. Test Instruments Required	Wireshark, UE + gNB simulator tool, OMC
4. Test Setup	Test Setup Small size 5G Core-2
5. Test Procedure	Action: • Perform configuration management task related to debugging/troubleshooting using management interface which is not publicly exposed Response: • Successful able to manage all action using management interface which is secured channel
6. Test Limits	NA
7. Expected Results	Management interface should be secured and accessible

1.Test No	GR_TSTP_6.1_D
2. Test Details	For performance management, the node shall generate various performance counters and provide mechanism to transfer the same to external entity for further analysis.
3. Test Instruments Required	Wireshark, UE + gNB simulator tool, OMC
4. Test Setup	Test Setup Small size 5G Core-2
5. Test Procedure	Action: • Perform downloading action of Performance KPI and related counter to local device Response: • Successful able to download performance related data
6. Test Limits	NA
7. Expected Results	External Download/transfer option should be enable for further debugging and troubleshooting

1.Test No	GR_TSTP_6.1_E
2. Test Details	Verification at OMC for the Fault report and alarm relate handling
3. Test Instruments Required	Wireshark, UE + gNB simulator tool, NMS (Network Management System) Testing Environment
4. Test Setup	Test Setup Small size 5G Core-2
5. Test Procedure	Action: • Perform action to generate alarm Situation and transfer to external/local device. • Configure situation/threshold to generate alarm at specific time/condition. Response: • Successful able to download externally alarm report which contain alarm type, Cause, Network Element and its type
6. Test Limits	NA
7. Expected Results	Successful able to capture all related information related to Fault and Alarm handling.

1.Test No	GR_TSTP_6.1_G
2. Test Details	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. Test Instruments Required	Wireshark, UE + gNB simulator tool, OMC
4. Test Setup	Test Setup Small size 5G Core-2
5. Test Procedure	Action: • Perform action to generate alarm Situation based out of threshold. Response: • Alarm Clears when condition/threshold meet automatically
6. Test Limits	NA
7. Expected Results	Successful able to clear Alarm based on threshold condition met.

1.Test No	GR_TSTP_6.1_H
2. Test Details	The NF shall support software upgrade.
3. Test Instruments Required	Wireshark, UE + gNB simulator tool, OMC
4. Test Setup	Test Setup Small size 5G Core-2
5. Test Procedure	Action: • Perform action to upgrade New release of software to upgrade functionality. Response: • Software version/patch upgraded successfully
6. Test Limits	NA
7. Expected Results	• Successful able to Upgrade/update software/ patch /version successfully

1.Test No	GR_TSTP_6.1_L
2. Test Details	Verify that system shall maintain a system log and core dump logs
3. Test Instruments Required	Wireshark, UE + gNB simulator tool, NMS (Network Management System) Testing Environment
4. Test Setup	Test Setup Small size 5G Core-2
5. Test Procedure	Action: • Perform action to enable logging at external server Response: • Successfully logging enable for system activity
6. Test Limits	NA
7. Expected Results	• Successful able to store system generated logging to external server

1.Test No	GR_TSTP_6.1_M
2. Test Details	Verification at OMC -The NF shall support alarms, events to OMC for visual indicators of status and fault.
3. Test Instruments Required	Wireshark, UE + gNB simulator tool, OMC
4. Test Setup	Test Setup Small size 5G Core-2
5. Test Procedure	Action: • Perform action on NF to generate alarm situation Response: • Able to see Alarm indication on GUI platform with respect to NF
6. Test Limits	NA
7. Expected Results	• Successful able to visualize alarm/Fault alarm with respect to NF element

1.Test No	GR_TSTP_6.1_N
2. Test Details	The NF shall have reboot and shut-down capability
3. Test Instruments Required	Wireshark, UE + gNB simulator tool, OMC
4. Test Setup	Test Setup Small size 5G Core-2
5. Test Procedure	Action: • Perform action to Shut down of specific network function. • Perform action to Reboot NF Response: • Shut down NF successfully • NF reboot successfully
6. Test Limits	NA
7. Expected Results	• Successful able to visualize alarm/Fault alarm with respect to NF element

1.Test No	GR_TSTP_6.1_O
2. Test Details	Verification at OMC -: Checks if the NF can provide system configuration data to the Management Information Base (MIB) of the system (applicable with SNMPbased management only).
3. Test Instruments Required	Wireshark, UE + gNB simulator tool, OMC
4. Test Setup	Test Setup Small size 5G Core-2
5. Test Procedure	Action: • Perform storage action of configuration files to database Response: • Successfully store Configuration files
6. Test Limits	NA
7. Expected Results	• Provision of system configuration data to the MIB (if applicable) is successful

GR/IR No.________________________________
TSTP No.________________________________
Equipment name & Model No.______________

Clause No.	***Compliance*** *(Complied /Not Complied / Submitted/Not Submitted / Not Applicable)*	***Remarks / Test Report Annexure No.***

[Add as per requirement]
Date:
Place: ***Signature & Name of TEC testing Officer /***
**** Signature of Applicant / Authorized Signatory***

**** Section J as given above is also to be submitted by the Applicant/ Authorised signatory as part of in-house test results along with Form-A. The Authorised signatory shall be the same as the one for Form 'A'.***