IMS TISPAN Architecture

GENERIC REQUIREMENTS
No.TEC/GR/SW ITA - 001/02/MAR- 10

(SUPERSEDES GR NO. GR/ ITA-01/01. MAR 2008)

TELECOMMUNICATION ENGINEERING CENTRE
DEPARTMENT OF TELECOMMUNICATIONS

TELECOMMUNICATION ENGINEERING CENTRE
DEPARTMENT OF TELECOMMUNICATIONS

IP MULTIMEDIA SUB-SYSTEM

GENERIC REQUIREMENTS

No.TEC/ GR/SW/ ITA - 001/02/ MAR-10

CONTENTS

TELECOMMUNICATION ENGINEERING CENTRE

DEPARTMENT OF TELECOMMUNICATIONS

IMS TISPAN Architecture

GENERIC REQUIREMENTS

No.TEC/ GR/SW/ ITA - 001/02/ MAR-10

HISTORY SHEET

S. No.	Title	GR No.	Remarks
1.	IMS TISPAN Architecture	GR/ ITA-01/01. MAR 2008	Issue 01
2.	IMS TISPAN Architecture	TEC/ GR/SW/ ITA - 001/02/ MAR-10	Issue 02

CHAPTER 1

Introduction

1.1 This Generic Requirement (GR) relates to IP Multimedia Sub-Subsystem (IMS), to deliver IP Multimedia (IM) services for wire-line as per TISPAN architecture, to be introduced in Indian Telecom Environment

1.2 This GR specifies the IMS architecture on the top of packet domain based on IP technologies and IETF protocols.

1.3 IP multimedia sessions shall use IP connectivity bearers. IP multimedia applications shall include content sharing, interactive gaming, real time multimedia applications, shared on line whiteboards etc.

1.4 TISPAN uses IMS specified by 3GPP to cater fixed line operators for end to end IP network for multimedia service.

1.5 For all ITU-T Recommendations, ETSI, 3GPP and IETF standards/ RFCs referred in this document, the latest release shall be applicable.

1.6 For all TEC documents referred in this document, the latest issue with all associated Amendments, Addendum and Corrigendum shall be applicable.

1.7 The network architecture shall enable the evolution of the IMS to 3GPP R7 to support Fixed Mobile Convergence.

1.8 The IP Multimedia Subsystem architecture shall support wide range of services enabled by the flexibility of Session Initiation Protocol (SIP).

1.9 Figure-1 shows a simplified version of TISPAN NGN architecture and figure-2 shows a simplified functional architecture.

CHAPTER 2

Description

2.1 Introduction to IMS

2.1.1 IMS is an end to end IP environment that provides seamless communication over IP.

2.1.2 IMS is a standard architecture developed by 3GPP that can be used by fixed, mobile and WI-FI operators. The IP Multimedia Subsystem (IMS) architecture will enable a mobile or fixed subscriber to use mobile and fixed multimedia services.

2.1.3 IMS provide a architecture separating the transport, control and application layer. The open architecture and platforms supported by IP and operating systems may lead to applications and new opportunities that are more difficult to replicate using a standard switched centralised solution.

2.1.4 SIP is used for the real-time, peer-to-peer, multi-party and multi-media capabilities of IMS.

2.1.5 IMS architecture defined by 3GPP is adopted by TISPAN for wireline networks and MMD for CDMA based networks defined by 3GPP2. However, in this document IMS is defined as per TISPAN.

2.1.6 TISPAN adds the NASS (Network attachment Subsystem) and RACS (Resource Admission Control).

2.1.7 The architecture must support of private and public user identification to enable users to enjoy multiple service at once.

2.1.8 The architecture also support FMC based or converged application likes Voice call continuity.

2.1.9 The IMS infrastructure and SIP Signaling is flexible enough to support a variety of telephony and non-telephony application servers.

2.2 General Requirement of Architecture

i) Common Core as per ES 282007 and applications.

ii) It shall be independent of underlying access technology.

iii) Support for strong control (General policies and Individual policies) imposed by the operator with respect to the services delivered to the end user.

iv) Support for rapid service creation without requiring standardisation (Standardising service capabilities instead of services). It shall also support faster deployment of new services.

v) Supports new applications such as presence information, video-conferencing, instant messaging, multi-party gaming, community services and content sharing.

vi) User profile is stored in a central location.

vii) Negotiable QoS for IP multimedia sessions both at the time of a session establishment as well as during the session by the operator and the user.

viii) The possibility for IP multimedia applications to be provided without a reduction in privacy, security or authentication

ix) Unique and customised applications leading to lower Capital Expenditure (CAPEX) and Operating Expenditure (OPEX).

x) The architecture shall support for easy scalability and redundancy.

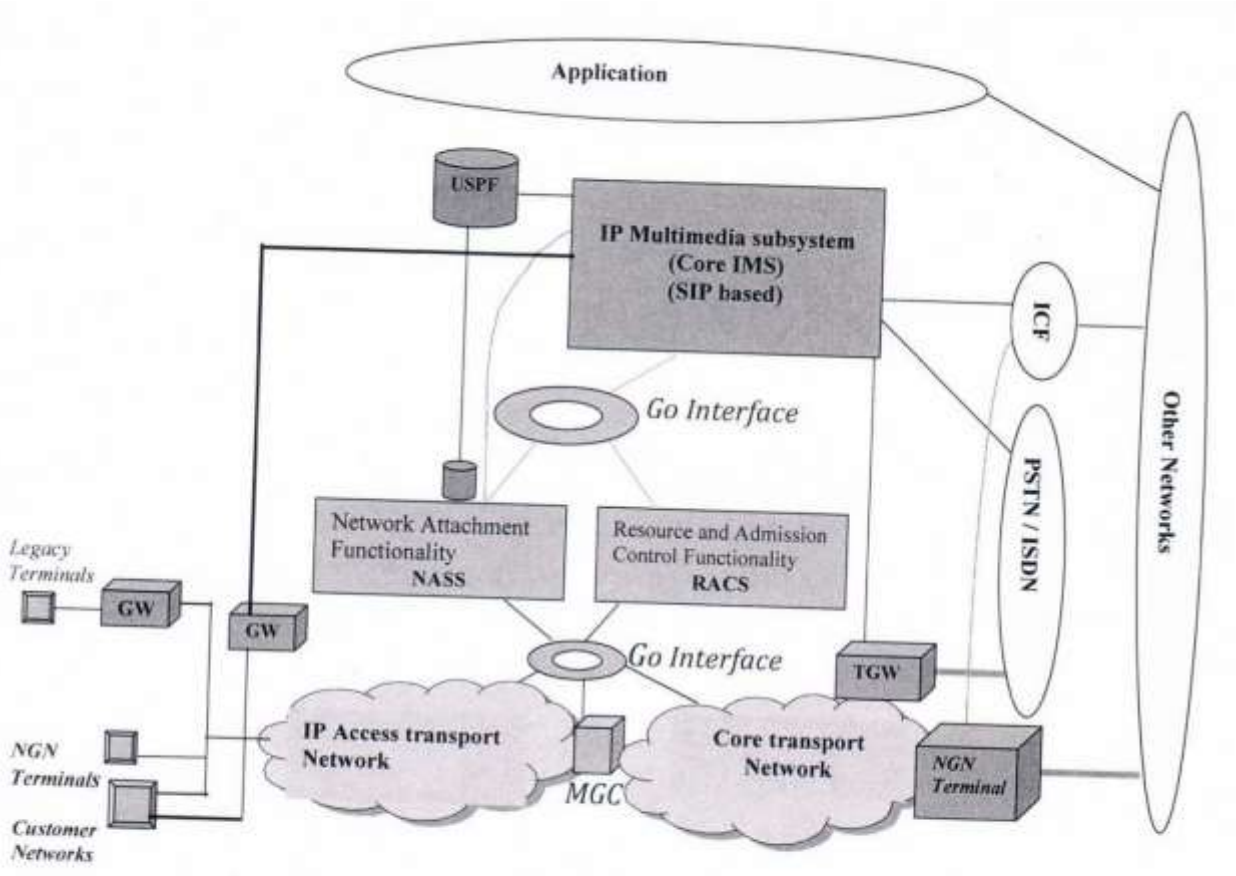

Figure 1: Simplified Version of TISPAN NGN Architecture

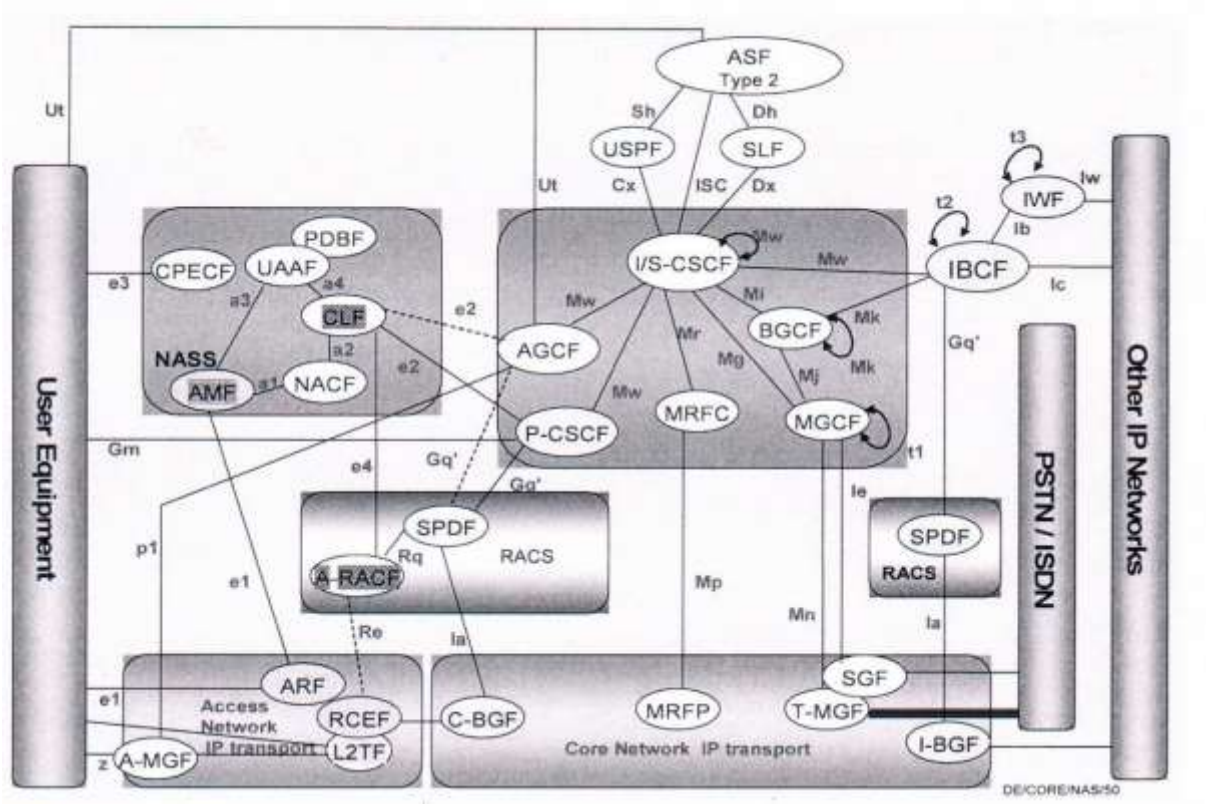

Figure 2 : A simplified functional architecture

Interfaces

a1	Interface between AMF and NACF
a2	Interface between CLF and NACF
a3	Interface between AMF and UAAF
a4	Interface between CLF and UAAF
Cx	Reference Point between a CSCF and an USPF
Dx	Reference Point between an I-CSCF and an SLF.
Dh	Reference Point between an AS and an SLF
e1	Interface between AMF and ARF
e2	Interface between CLF and P-CSCF
e3	Interface between CPECF and UE
e4	Interface between CLF and A-RACF

Gm	Reference Point between a UE and a P-CSCF.
Gq’	Reference Point between a SPDFand a P-CSCF/AGCF
ISC	Reference Point between a CSCF and an Application Server.
Ia	Reference Point between IWF and other IP network
Ic	Reference Point between IBCF and other IP network
Iw	Reference Point between IWF and other IP network
Ie	Reference Point between MGCF and SGF
Ib	Reference Point between IWF and IBCF
Mg	Reference Point between an MGCF and a CSCF.
Mi	Reference Point between a CSCF and a BGCF.
Mj	Reference Point between a BGCF and an MGCF.
Mk	Reference Point between a BGCF/IMS ALG and another BGCF.
Mn	Reference Point between a MGCF and an IP multimedia network
Mp	Reference Point between a MRFC and an IP multimedia network
Mr	Reference Point between an CSCF and an MRFC.
Mw	Reference Point between a CSCF and another CSCF.
p1	Reference Point between a A-MGF and AGCF
Re	Reference Point between A-RACF and RCEF
Rq	Reference Point between A-RACF and SPDF
Sh	Reference Point between USPF and AS
t1	Interface at MGCF
t2	Interface at IBCF
t3	Interface at IWF
Ut	Reference Point between UE and an Application Server.
Z	Reference Point between UE and an A-MGF

2.3 Application server Requirement

2.3.1 The Application server shall host and execute services and interfaces with S-CSCF using SIP.

2.3.2 The Application server allows third party providers an easy integration and deployment of their value added services to the IMS infrastructure.

2.3.3 Depending on the actual service, the AS can operate in SIP proxy mode, SIP UA (user agent) mode or SIP B2BUA (back-to-back user agent) mode.

2.3.4 An Application server can be located in the home network or in the external third party network.

2.3.5 TEC GR No. GR/SAS-01 shall be referred for additional functionality of Application Server.

2.4 Media Resource Functionalities Requirement

The MRF shall provide specialized media resources including

- Digit detection
- Announcement playback and recording
- Media mixing functions such as 3 to 6- party call conferencing
- Video media such as video greeting and video attendant

Media resource function has mainly two part namely 1) MRFC and 2) MRFP

2.4.1 Media Resource Function Controller (MRFC) Requirement

i). The MRFC shall be aligned with the functionality as specified in ETSI TS 123 002

ii). The MRFC can be stand alone or integrated with AS.

iii). MRFC shall support Mp interface towards MRFP

iv). The Mp interface shall be based on ETSI TS 123 002 .

2.4.2 Media Resource Function Processor (MRFP) Requirement

i). The MRFP shall be aligned as specified in ETSI TS 123 002

ii). The MRFP is a standalone element of the IMS platform.

iii). The MRFP shall have the capabilities to control the following:

a) Playing audio and video announcements
b) Audio and video trans-coding
c) Voice prompts
d) DTMF detection
e) Tone generation
f) Recording
g) Media mixing for conf. Calls

MRFP must transport payload via RTP to other entities as described in ETSI TS 123 002

2.4.3 CODEC SUPPORT

The following codec (but not limited to the following) shall be supported

G.711 A - law

G.726

G.726 A

G.727

G.729

H.261

H.263

H.264

Any addition to above any other codecs as per ITU-T recommendation shall also be supported .

2.5 Break-out Gateway Control Function support (BGCF)

BGCF, a SIP server, shall interact with S-CSCF, MGCF and peer BGCFs in external IMS networks. BGCF shall be used for routing a call from IMS to PSTN/PLMN or UMTS and support following requirement

2.5.1 BGCF shall support the Mi interface, between the BGCF and the S-CSCF according to TS 123.002.

2.5.2 BGCF shall support the Mj interface, between the BGCF and the MGCF according to TS 123.002.

2.5.3 BGCF shall support the Mk interface, between the BGCF and another BGCF according to TS 123.002.

2.5.4 BGCF shall receive request from S-CSCF to select appropriate PSTN/PLMN Domain break out point for the session.

2.5.5 BGCF shall select the network in which the interworking with the PSTN/PLMN Domain is to occur. If the interworking is in another network, then the BGCF shall forward the SIP signalling to the BGCF of that network.

2.5.6 BGCF shall select the MGCF in the network in which the interworking with PSTN/PLMN domain is to occur and forward the SIP signalling to that MGCF. This shall not apply if the interworking is a different network.

2.6 PSTN Gateways Requirements

PSTN gateway interfaces with PSTN circuit switched (CS) networks. For signalling, CS networks use ISUP over MTP while IMS uses SIP over IP. For media, CS networks use PCM while IMS uses RTP. It support following parts:

Signalling gateway (SGW): It interfaces with the signalling plane of the circuit switched network. It transforms the lower layer protocols as SCTP (which is an IP protocol) into MTP (which is a SS7 protocol) to pass ISUP from the MGCF to the CS network and have minimum following functionalities

i) It shall be possible to extract and process the signalling information

ii) It shall support M3UA transport over SCTP.

iii) The signalling gateway shall be able to handle signalling traffic load up to 0.4 Erlang per signalling link including signalling traffic due to failure of other standby signalling links.

2.7 Media Gateway (MGW) & Media Gateway Control Function (MGCF) Requirement

i) MGCF shall support Mg interface to CSCF and associated functional behavior.

ii) It shall have the flexibility to co-locate SGW and IM-MGW in one node in case conversion of transport for signaling is needed locally.

iii) The MGCF shall control the media gateways using the H.248 control profile as per ES 283024.

iv) The H.248 shall be transported using SCTP or UDP.

v) The MGCF shall support text encoding in ABNF format.

2.8 Network attachment Subsystem (NASS)

2.8.1 The functional architecture shall be as per ETSI specification ES 282 004.

2.8.2 Following logical functions for NASS shall be supported.

- NACF (Network access configuration Function) is either DHCP or RADIUS server
- AMF (Access management function) is either a RADIUS client or a DHCP relay
- CLF (Connectivity session location and Repository Function) is a location database
- PDBF (Profile Database Function) is user profile database
- CNG (Customer Network gateway) is a RGW or LAD

2.8.3 The NACF shall support the IP address allocation and may distribute DNS and P-CSCF addresses

2.8.4 The AMF shall translate network access request into appropriate NACF and UAAF transactions

2.8.5 The PDBF shall contain user authentication data (user identity and list of supported authentication methods) and information related to the required network access configuration. This is referred to as “subscriber QoS profile”

2.8.6 PDPF shall support implementation of a Subscriber Profile database that contains associations between services and network resources, for example, bandwidth capacity and QoS tied to layer 2 constructs such ATM VC/VP, Ethernet line ID and VLAN.

2.8.7 The CLF shall register and maintain the association between the IP address allocated to the UE and related network information (for example, the physical access circuit)

2.8.8 The CLF passes the IP address, location and (potentially) subscriber QoS profile to the A-RACF to allow for subscriber identification over the Rq interface.

2.8.9 The CLF shall associate user identity, IP address, network location info (e.g line ID) and geographical location.

2.8.10 The following main interface shall be supported:

- a2 (NACF-CLF) Diameter
- e4 (CLF-A-RACF) Diameter
- e2 (CLF-P-CSCF) Diameter
- Rq (S-PDF-A-RACF) Diameter

2.9 Resource and Admission Control Substem (RACS)

2.9.1 The functional architecture shall be as per ETSI specification ES 282 003

2.9.2 The RACS must support fixed mobile and cable access network.

2.9.3 The under mentioned main logical functions for RACF shall be supported:

- AF (Application Function) is collocated in P-CSCF
- SPDF (Server Based Policy decision Function)
- C-BGF (Core–Border gateway Function) is in session Border Controller.
- A-RACF (Access- Resources and admission Control function)
- RCEF (Resource Control Enforcement Function) is in Edge router

2.9.4 The A- RACF shall support:

- Use the Qos information received from the SPDF to perform admission control i.e. it check whether the requested QoS resources can be made available for the relevant access network.

- Use network policies to authorise a resource reservation request against a particular access line

- Enforce admission control decision by setting L2/L3 QoS policies in the RCEF via Re to police user traffic. Re interface shall be supported as and when standardized is completed by TISPAN.

2.9.5 The SPDF shall support:

- Policy decision using rules for Service Based Policy Control (SBP)

- Request approval of resource reservation requests from the A-RACF

- Communication with the Border Gateway Function (BGF) for gate control, far-end NAT traversal and NAT/FW control

2.9.6 The C-BGF shall enforce policies and performs NAPT-PT functionality under control of the SPDF and support:

- gate Control

- packet marking

- NAPT-PT

- Hosted NAT traversal

- Policing of down/uplink traffic

- Usage metering

2.9.7 The AF shall support:

- Request authorization of bearer resources from the SPDF

- Request bearer resources to be reserved for a session

- Receive notifications when resources are reserved and released.

2.9.8 The RCEF shall enforce policies under the control of the A-RACF and support

- gate control

- packet marking

- traffic policing

2.10 Charging

2.10.1 IM CN sub-system functional elements shall provide support for offline and online charging including support for charging correlation e.g. between IM CN sub-system and PS domain.

2.10.2 The charging data sent by the IMS nodes shall contain the identification of the originating and terminating user in order to be identified by the Charging Collection Function (CCF)/ OSC.

2.10.3 The collection of charging information from the nodes shall be done through the DIAMETER protocol.

2.10.4 The on-line charging at Ro interfaces & off-line at RF interfaces shall be in accordance to ETSI TS 132.260.

2.10.5 The CCF shall support FTP over TCP/IP or FTAM over TCP/IP for the CDR transfer.

2.10.6 The CCF node shall format and assemble the CDR's and support ASN.1/BER encoding, XML,ASCII formats.

2.10.7 Online charging architecture shall be supported..

2.10.8 The real time charging interface nodes shall be based on Diameter Credit Control Application (DCCA).

2.10.9 The nodes shall support p-charging vector field for OFF line system to correlate.

2.11 CORE NODE

The most important of the core node is the Call Session Control Function (CSCF), also known as a SIP server. CSCF is the central routing engine and policy enforcement point for the network and uses the SIP protocol for call control. Support of three types of CSCFs required are P-CSCF, I-CSCF and S-CSCF

The entities shall be either co-located or standalone mode based on network configuration.

2.11.1 The P-CSCF, I-CSCF and S-CSCF shall conform to ETSI TS 124.229 and ETSI TS123.228.

2.11.2 The CSCF shall support the forwarding of SIP messages, according to SIP method, registration status of the relevant subscriber and appropriate routing mechanism (ENUM, DNS, pre-defined route).

2.11.3 The CSCF shall support IPv4 as well as IPv6

2.11.4 The CSCF shall support both TCP and UDP as transport protocols.

2.11.5 CSCF shall comply with the following standards:

- DES-02029-NGN-R1 NGN Core IMS Architecture
- DES-02032-NGN-R1 Charging
- DTS-03022-NGN-R1 NGN Call Diversion (CDiv)= call forwarding

Proxy-CSCF (P-CSCF): The P-CSCF handles all of the requests to/from the user and forwards them to appropriate Interrogating-CSCF (I-CSCF). The main functions of P-CSCF are:

2.11.6 The P-CSCF shall support the Mw interface to the I-CSCF and S-CSCF, compliant to ETSI TS 124.229.

2.11.7 The P-CSCF shall support the Gm interface to the UE, compliant to ETSI TS 124.229.

2.11.8 The P-CSCF shall be able to determine the address of the I-CSCF .

2.11.9 The P-CSCF shall be able to forward SIP messages received from the UE to the SIP server (e.g. S-CSCF) discovered during registration procedure.

2.11.10 The P-CSCF shall be able to forward the SIP request or response to the UE.

2.11.11 The P-CSCF shall be capable to discard any received SIP message that is not integrity protected and received outside of the authentication and registration procedure.

Interrogating-CSCF (I-CSCF): It queries to obtain the address of appropriate Serving CSCF (S-CSCF) where the request must be forwarded.

2.11.12 The I-CSCF shall support the Mw interface to the P-CSCF and the S-CSCF, compliant to ETSI TS 1 24.229.

2.11.13 The I-CSCF shall support the Cx interface to the USPF, compliant to ETSI TS 129.228 & ETSI TS 129.229.

2.11.14 The I-CSCF shall support the Dx interface to the SLF, compliant to ETSI TS 129.228 & ETSI TS 129.229.

2.11.15 The I-CSCF shall be able to select an appropriate S-CSCF depending upon S-CSCF capabilities for a subscriber performing SIP registration, during the registration procedure.

2.11.16 The I-CSCF shall route a SIP request received from another network towards the S-CSCF.

2.11.17 The I-CSCF shall obtain the address of the S-CSCF.

2.11.18 The I-CSCF shall forward the SIP request or response to the S-CSCF.

Serving CSCF (S-CSCF): It routes the SIP Signalling to and from subscribers via Application servers, as per the service profile information for each subscriber. The S-CSCF uses DIAMETER protocol (Cx and Dx interfaces) to download user profiles and inform S-CSCF address & user states. It has no local storage of the user information. The main functions of S-CSCF are:

a. Enforces the policy of the network operator.

b. SIP registration

c. SIP message routing

d. Service usage authentication & authorisation

2.11.19 The S-CSCF shall support the ISC interface to Application Servers, compliant to ETSI TS 124.229.

2.11.20 The S-CSCF shall support the Cx interface to the USPF, compliant to ETSI TS 129.228 and ETSI TS 129.229.

2.11.21 The S-CSCF shall support the Mw interface to the P-CSCF and I-CSCF, compliant to ETSI TS 124.229.

2.11.22 The S-CSCF shall support the Mg interface to other S-CSCFs, compliant to ETSI TS 124.229.

2.11.23 The S-CSCF shall support the Mr interface to MRFC, compliant to ETSI TS 124.229.

2.11.24 The S-CSCF shall support the Rf interface to the CCF, compliant to ETSI TS 132.260.

2.11.25 The S-CSCF shall support the Ro interface as per ETSI TS 132.260 which defines IMS-GWF between S-CSCF and OCS. The interface between S-CSCF & IM-GWF is 'ISC' and 'Ro' between IM-GWF and OCS in interface is 'Ro'.

2.11.26 S-CSCF shall generate charging information for the following events:

i) Connection of a session

ii) Release of a session

iii) Event during a session

2.11.27 It shall be configurable to enable or disable the generation of an ACR message by the IMS node in response to a particular ;Triggering SIP Method/ISUP

Message'

2.11.28 The S-CSCF shall support the ability to configure the periodic re-registration timer.

2.11.29 The S-CSCF shall support Initial Filter Criteria with priorities assigned to it.

2.11.30 The S-CSCF shall support the capability to send a third party registration request to an Application Server.

2.11.31 The S-CSCF shall be able to behave as a SIP Proxy. The mechanisms followed shall be in accordance with ETSI TS 124.229.

2.11.32 The S-CSCF shall be able to behave as a SIP Registrar for all SIP User Agents belonging to the IMS Core Network subsystem and with public user identities not barred by the IMS Core Network. The mechanisms followed shall be in accordance with ETSI TS 124.229.

2.11.33 The S-CSCF shall be capable of using binding information based on the IP address, Public and Private User Identities of the UE for authentication and authorization purposes.

2.11.34 The S-CSCF shall support the ability to translate E.164 addresses to a SIP routable SIP URI using an ENUM DNS translation mechanism as per RFC 3761. If this translation fails, then the session shall be routed to the PSTN

2.11.35 The S-CSCF shall be compliant with the SDP usage defined in ETSI TS 124.229. Supported mechanisms to perform the same shall also be provided.

2.11.36 The S-CSCF shall be able to provide charging information, describing an IMS session to the CCF which will then generate the CDR.

2.11.37 The S-CSCF shall perform the following functions during a session

i) Registration

ii) Session-related and session-unrelated flows

iii) Charging and resource utilisation

2.12 USPF

The USPF is the master database for a given user. It is the entity containing the subscription-related information to support the network entities actually handling calls/sessions.

2.12.1 TheUSPF shall fully provide the functionality of IM CN sub-system specified in ETSI TS 123.002.

2.12.2 The USPF shall support call and/or session establishment support according to ETSI TS 123.002 in the IM CN sub-system in PS Domain. For terminating

traffic, it shall provide information on which call and/or session control entity currently hosts the user.

2.12.3 The USPF shall keep the appropriate relations between the private identity identifying the IMS user (i.e. Network Access Identifier-NAI,) and the public identities used for session establishment (i.e. SIP_URI, TEL_URL).

2.12.4 USPF shall be able to generate user authentication, integrity and ciphering data for the PS Domains and for the IM CN sub-system.

2.12.5 It shall be possible to support multiple service profiles per user as per ETSI TS 123.228.

2.13 IMS ALG Requirement

2.13.1 The IMS ALG shall communicate between IPv6 and IPv4 SIP applications.

2.13.2 The IMS ALG shall request NA(P)T-PT to provide the binding data between the different IP addresses (IPv6 to IPv4 and vice versa) upon session initiation and shall release the bindings at session release.

2.14 Naming and Addressing

2.14.1 The IMPI (IMS Private Identity) identities of the user shall be in accordance to ETSI TS 123.003.

2.14.2 The system shall support both SIP-URI and TEL-URI user identity formats.

2.14.3 The system shall support RFC 3263 (Locating SIP Servers).

2.14.4 Every IM CN subsystem user shall have one or more Public User Identities.

2.14.5 A Public User Identity/identities shall be registered either explicitly or implicitly before the identity can be used to originate IMS sessions and IMS session unrelated procedures as per ETSI TS 1 23.228.

2.14.6 Public User Identity/identities shall be administered by the network operator and shall not be changeable by the user shall as per ETSI TS 123.228.

2.14.7 Public User Identity/identities shall be authenticated by the network during initial registration and optionally on subsequent registration as per ETSI TS 123.228.

2.14.8 Private User Identity/identities shall take the form of a Network Access Identifier (NAI) as defined in RFC 2486.

2.14.9 The Private User Identity/identities are not used for routing of SIP messages as per ETSI TS 123.228.

2.14.10 Routing of SIP signalling within the IMS shall use SIP URIs or tel URI, as per ETSI TS 123.228.

2.14.11 E.164 format Public User Identities shall not be used for routing within the IMS. Session requests based upon E.164 format Public User Identities will require conversion into SIP URI format for internal IMS usage.

2.14.12 The relationships between private and public user identities and between user identities and service profiles shall be as per ETSI TS 123.228.

2.14.13 All core IMS network nodes (e.g. x-CSCF, BGCF, MGCF,) shall be identifiable using a valid SIP URI (Host Domain Name or Network Address) on those interfaces supporting the SIP protocol as per ETSI TS 123.228.

2.14.14 The SIP URIs of the network nodes shall be used when identifying these nodes in header fields of SIP messages.

2.14.15 The S-CSCF needs to obtain and store a Private User Identity upon registration and unregistered termination in accordance to ETSI TS 123 228.

2.14.16 Routing of SIP signalling within the IMS shall use SIP URIs or other (non SIP) in accordance to ETSI TS 123 228.

2.15 Supplementary services

2.15.1 The architecture shall support the supplementary services as per ETSI TS 181.002.

2.15.2 The architecture shall support the supplementary services mentioned in TEC standard no. TEC/SR/NSF-SU2/01 JAN09.

2.15.3 All service feature shall be usable for on-net SIP-SIP/IMS-IMS) as well as off net (IMS-PSTN/PSTN-IMS).

2.15.4 The service shall be available for both pre- paid and post paid subscriber

2.16 PSTN/ISDN EMULATION

2.16.1 The goal of this emulation is to provide a means to implement PSTN and ISDN features for TDM based phones in an NGN based approach. The emulation can be achieved by any of the following method to support all narrowband access ; V5.2,ISDN PRI, ISDN BRI and POTS.

a) As per ETSI ES 282.001

b) As per ETSI TS 182. 012

CHAPTER 3

FUNCTIONAL REQUIREMENTS

3.1 General

3.1.1 The IMS core network is to provide users a wide range of IMS application & services. The technology shall facilitate evolution towards Next Generation systems.

3.1.2 Expansion of the system shall be modular.

3.1.3 The equipment shall be fully solid state and adopt the state of the art proven technology. The equipment shall have the following features:

i). Low power consumption

ii). Minimum number of power supply's voltages in the equipment

3.2 Support of Multiple Equipment vendors

The IMS Core network shall support the possibility of integrating to the existing FIXED LINE infrastructure, without any restriction.

3.3 Operational Requirement (OR): The system shall meet the following maintenance & operational requirements:

i) The design of the equipment shall not allow plugging of a module in the wrong slot or upside down.

ii) The removal or addition of any interface cards shall not disrupt traffic on other cards.

iii) All critical modules shall be identified and shall be provided in full redundant configuration.

iv) Suitable Visual indication shall be provided for displaying healthy, unhealthy operation conditions.

v) A single point failure on the equipment shall not result in network or network management system downtime.

vi) In the event of a bug found in the software, the manufacturer shall provide patches and firmware replacement if involved, free of cost. Compatibility of the existing hardware shall be maintained with future software/firmware.

vii) In the event of a full system failure, a trace area shall be maintained in non-volatile memory for analysis and problem resolution.

viii) A power down condition shall not cause loss of connection configuration data storage.

ix) Live Insertion and hot swap of modules shall be possible to ensure maximum network availability and easy maintainability.

x) The Hardware and software components shall not pose any problems in the normal functioning of all network elements wherever interfacing with Service Provider's network for voice, data and transmission systems, as the case may be.

xi) The equipment shall have availability figure of 99.999%. The MTBF (Mean Time Between Failure) and MTTR (Mean Time To Restore) Predicted and observed values shall be furnished along with calculations by the manufacturer.

3.4 Faults and Event Management (FM)

3.4.1 A centralised fault and event database, with atleast the following fault and event management functions, shall be provided :

i) Store and display the real time alarm status and alarm history (for atleast one month which shall be configurable by service provider) of all network entities. It shall be possible to configure the number and size of log files in order to define the duration for which data is kept and to avoid storage overflow.

ii) Detect improper behaviour of the network resources.

iii) Send fault (alarm and event) data automatically.

iv) Decide through the terminal which alarms and events are displayed on the screen.

v) State the reason of alarms or event and the possible actions for the user in the same on-line customer documentation.

vi) Allow the node to keep track of its own problems so as to allow a multi-manager environment making the network safe from loss of data caused by temporary management or data link problems as well as management terminal failures.

vii) Automatically clear the alarms and events in the files when the problem is solved and the clearance of alarm.

viii) Be able to filter the alarms and events, at IMS component level, according to date, time, alarms class (e.g. critical, major, minor and warning)

ix) Allow the management via the command line interface and allow the external management equipment to get alarms via an SNMP/ CORBA interface

3.5 Performance Management

3.5.1 A centralised performance measurement database with atleast the following functionality shall be provided:

i) Administration of the user-defined performance measurement e.g. traffic measurement and processor load measurement.

ii) Administration of statistical data and performance trends for all types of alarms and network measurement counters in a commercially available database (e.g. Oracle) and backup of alarm and performance data.

iii) Real-time observation used to implement foreground real-time data acquisition and display.

3.5.2 Performance Management system shall allow for measuring, storing, monitoring & alarming and forwarding all relevant performance counters of the IMS components.

3.5.3 There shall be an interface between Performance and Fault Management system to allow for issuing alarms and clear events when configurable thresholds of performance counters are met.

3.5.4 It shall be possible to filter performance data.

3.5.5 For every logical function and interface, which is provided by the IMS system in terms of being an enabling system for applications and services, atleast but not limited to following shall be available:

i) capacity, e. g. queue levels, etc.

ii) usage, e. g. transactions per second, concurrent sessions, etc.

iii) answering performance, e. g. session setup time, latency, etc.

iv) availability, e. g. per day

It shall be possible to measure, store, monitor and forward the above parameters.

3.6 Configuration Management (CM)

3.6.1 The Configuration Management (CM) shall be available to:

i) allow the operator to set, modify and examine hardware and software configuration parameters and configuration files for the IMS nodes.

ii) provide software management (i.e. to control what software is installed where and in which version).

iii) provide equipment management and application configuration in general.

3.6.2 It shall be possible to perform In-Service Maintenance, i. e. applying new

software or configuration without causing service outages or data loss, e. g. by supporting two different software/configuration versions running simultaneously on the IMS components or similar.

3.6.3 It shall be possible to revert to earlier versions of software and configuration versions on the offered OMC platform, IMS elements and application services.

3.6.4 CM shall configure IP connectivity, connectivity and server invocation configuration for internal SIP signalling and Diameter connections between nodes.

3.7 Backup and recovery

3.7.1 A redundant local backup (i.e. hard disk) for the following purposes shall be provided:

i) System software backup

ii) Alarm log and internal error log backup

iii) Event log (CM, PM, FM) backup

iv) System configuration backup

v) Charging data backup

It shall be possible to take back-up for atleast seven days of operation. While taking or loading back-up data, it shall be possible to recover the services within 30 minutes and full normalcy of the system shall be within four hours.

3.7.2 Accounting and authorisation shall be performed before granting access to the system.

3.7.3 It shall be possible to differentiate between levels of access rights for administrator, operator ,users etc.

3.7.4 It shall be possible to follow unsuccessful logins. A maximum value for them shall be possible to set, after which a given account shall be locked.

3.7.5 It shall be possible to change all password in the system. It shall be possible to define a time interval to force the user to change the password.

3.7.6 It shall not be possible to monitor the clear text value of a static password while en-route over the network and stored.

3.7.7 It shall be possible to automatically logout the user session after a certain time period (inactivity timeout).

3.7.8 Administrative access must be done using protocols such as SSHv2.

3.7.9 The system shall keep a log of user and performed operations.

3.8 SIP signaling with HTTP Digest Authentication

- The system shall identify the client (i.e. IETF SIP UA) using the 'To' header field in the SIP Register message as described in RFC 3261. This field contains the address-of-record (AOR) of the client, that is, the public user identity.

- The system shall authenticate an identified client using the HTTP Digest Authentication mechanism described in RFC 2617.

3.9 NASS-IMS Bundled Authentication

This shall be supported as defined by TISPAN R1. It shall provide a Single Sign-On authentication mechanism that allows the re-use of the access authentication and security from the fixed access network to authenticate the users when accessing the IMS system.

3.10 Audit functions

Error detection programs, which run periodically or on demand in the background, shall be provided. Such audit functions shall periodically poll the status of the cards, links and other connection related status and report them. Audits shall also be configured to identify hung call related contexts and clear them.

3.11 Audit Trail Recording

Audit trail recording (logging) must be used in the system to enable detection of suspicious network and user activity. The audit trail recording covers logging of both the traffic and the management related events. Filtering must be possible to apply in order to reduce the sizes of the log files. The system must provide methods for storing the logs files securely.

CHAPTER 4

INTERCONNECTIVITY AND INTEROPERABILITY REQUIREMENTS

4.1 Interfaces and Protocol

The various under mention interfaces and protocol shall be fully compliant to TISPAN standards and shall operate in a multi-vendor environment.

S.no.	TISPAN Interface	TISPAN Protocol
1.	Gm	SIP
2.	Mw	SIP or SIP-I
3.	Mr	SIP
4.	Mg	SIP or SIP-I
5.	Mi	SIP or SIP-I
6.	Mj	SIP or SIP-I
7.	Mk	SIP-I or SIP
8.	ISC	SIP-I or SIP
9.	Ib	SIP-I ou SIP
10.	Ic	SIP-I or SIP
11.	Iw	H.323 or SIP
12.	Ie	SSURN/SSURF over SIGTRAN
13.	t1	SSURN/SSURF over SIGTRAN
14.	t2	SIP or SIP-I
15.	t3	H323 or SIP
16.	Ut	HTTP/XCAP
17.	Dh	DIAMETER
18.	Dx	DIAMETER
19.	Cx	DIAMETER
20.	Gg’	DIAMETER
21.	Sh	DIAMETER
22.	P1	H.248
23.	Mn	H.248
24.	Mp	H.248
25.	Ia	H.248

26.	Rq	DIAMETER
27.	Re	Non applicable
28.	e1	DHCP
29.	e2	DHCP
30.	e3	To be determined
31.	e4	To be determined
32.	a1	DHCP
33.	a2	To be determined
34.	a3	Radius/ DIAMETER
35.	a4	To be determined
36.	z	Analog interface

The core shall support dual stack IPv4/ IPv6.

4.2 Requirement Of Interworking With ENUM

4.2.1 ENUM shall be support as per RFC 3761.

4.2.2 All the Tel-URI formats viz. international, national, local format shall be supported.

4.2.3 It shall be possible to route SIP INVITE (VoIP) dialogues which can not be resolved to a fixed system address by default to a special component (MGCF in case of received PSTN/PLMN network number URL.)

4.2.4 DNS NAPTR record types, as per RFC 2915 shall be are supported.

4.2.5 The ENUM server shall be integrated in the DNS server or can be separate entity.

4.2.6 Redundancy shall be provided for the ENUM server.

4.2.7 The system shall support iterative and recursive queries.

4.3 Requirement of IMS interworking with DHCP

4.3.1 The DHCP server shall support IPv4 as well as IPv6.

4.3.2 The DHCP server shall support dynamic DNS update mechanism.

4.3.3 The DHCP server shall operate as per IETF RFC 2131: Dynamic Host Configuration Protocol and IETF RFC 3315: Dynamic Host Configuration Protocol for IPv6:RFC 3319 'Dynamic Host Configuration Protocol (DHCPv6) Options for Session Initiation Protocol (SIP) Servers' & RFC 3646 'DNS

Configuration options for Dynamic Host Configuration Protocol for IPv6 (DHCPv6)'.

4.3.4 Updates sent to the name server must be secured and shall not be sent by the UE but by the network component (GGSN/AAA server/DHCP server).

4.4 Tispan Inter working

4.4.1 The functional architecture for interworking with other networks shall be supported as defined by TISPAN and shown in below figure 3:

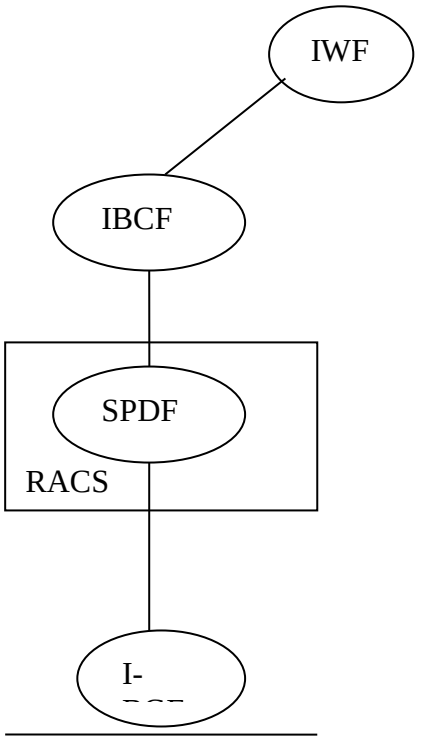

Figure 3 : A simplified functional architecture

4.4.2 The Interconnect Border Control Function (IBCF) shall:

- Provide application specific functions at the SIP/ SDP protocol layer in order to perform interconnection between two operator domains.
- Support communication between Ip v6 and IP v4 SIP applications

- Support network topology hiding, screen SIP signalling information, select the appropriate signalling interconnect and also support generation of charging data records.

4.4.3 Inter- working Function (IWF) shall provide signalling protocol inter-working between the SIP-based IMS network and other service provider networks.

4.4.4 Interconnect Border Gateway Function (IBGF) shall:

- Support pinhole firewall and NAT to protect the service provider's IMS core.
- Controls access by packet filtering on IP address/port and opening/closing gates (pinholes) into the network.
- Use Network Address and port Translations (NAPT) to hide the IP addresses/ports of the service elements in the IMS core.
- Support QoS packet marking, bandwidth & signalling rate policing and QoS measurements for the media flows
- Support also Topology Hiding Inter-network Gateway function.

CHAPTER 5

QUALITY REQUIREMENTS

5.1 Quality of Service (QoS)

5.1.1 The systems shall support policy based control of Laye2/3 resources in access network for guaranteeing QoS. The functional architecture is shown in figure 4 given below:

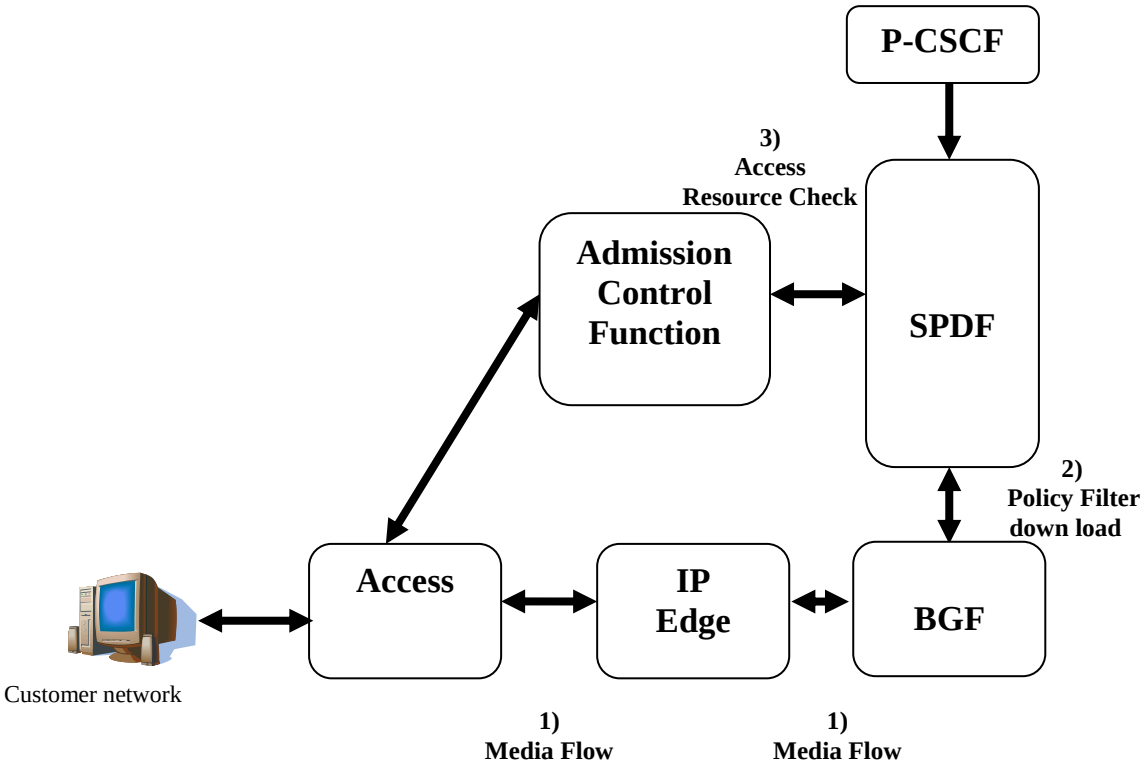

Figure 4 : A simplified functional architecture

5.1.2 The QoS authorisation and enforcement shall be done in alignment with the TISPAN model.

The QoS authorisation shall be done as mentioned below:

- The P-CSCF (AF) shall derive the flow description from SDP (media type, bandwidth, service identifier) in the SIP signalling.

- The flow description shall be sent to the SPDF (Session Policy Decision Function).

- SPDF shall requests the A-RACF (Access Resource Admission Control Function) to check if there are available resources in the access network.

- If there are resources a filter matching the flow Description and the relevant policy is downloaded in the Border Gateway Function (BGF) node.

The QoS enforcement shall be done as mentioned below:

- The BGF (Border Gateway Function) shall open/close uplink and downlink flow gates in line with the SDP and session state information available in the Filter Information downloaded from P-CSCF via SPDF (session Policy Decision Function) on a per session basis.

- The BGF shall do the bandwidth policing in downlink and uplink direction.

- Uplink Diffserv marking (DSCP) policy enforcement shall be done on a per media flow basis. The DSCP value to be used shall be downloaded to BGF as part of the flow filter. Diffserv policies shall involve media flow type and service identity.

- For QoS in the IP core network, the routers shall Diffserv and IP/MPLS (Optional)

CHAPTER 6

Electromagnetic Compatibility (EMC) Requirements

6.1

General Electromagnetic Compatibility (EMC) Requirements: - The equipment shall conform to the EMC requirements as per the following standards and limits indicated therein. A test certificate and test report shall be furnished from a test agency.

a) Conducted and radiated emission *(applicable to telecom equipment)*:

Name of EMC Standard: "CISPR 22 (2005) with amendment 1 (2005) & amendment 2 (2006) - Limits and methods of measurement of radio disturbance characteristics of Information Technology Equipment".
Limits:-

i) To comply with Class A (to be mentioned in the GR / IR as per the specific requirement) of CISPR 22 (2005) with amendment 1 (2005) & amendment 2 (2006).

ii) The values of limits shall be as per TEC Standard No. TEC/EMI/TEL-001/01/FEB-09**.**

b) Immunity to Electrostatic discharge:

Name of EMC Standard: IEC 61000-4-2 {2001) "Testing and measurement techniques of Electrostatic discharge immunity test".

Limits: -

i) Contact discharge level 2 {± 4 kV} or higher voltage;

ii) Air discharge level 3 {± 8 kV} or higher voltage;

c) Immunity to radiated RF:
Name of EMC Standard: IEC 61000-4-3 (2006) "Testing and measurement techniques-Radiated RF Electromagnetic Field Immunity test"

Limits:-

For Telecom Equipment and Telecom Terminal Equipment with Voice interface (s)

i) Under Test level 2 {Test field strength of 3 V/m} for general purposes in frequency range 80 MHz to 1000 MHz and

ii) Under test level 3 (10 V/m) for protection against digital radio telephones and other RF devices in frequency ranges 800 MHz to 960 MHz and 1.4 GHz to 6.0 GHz.

For Telecom Terminal Equipment without Voice interface (s)

Under Test level 2 {Test field strength of 3 V/m} for general purposes in frequency range 80 MHz to 1000 MHz and for protection against digital radio telephones and other RF devices in frequency ranges 800 MHz to 960 MHz and 1.4 GHz to 6.0 GHz.

d) Immunity to fast transients (burst):

Name of EMC Standard: IEC 61000- 4- 4 {2004) "Testing and measurement techniques of electrical fast transients/burst immunity test"

Limits:-

Test Level 2 i.e. a) 1 kV for AC/DC power lines; b) 0. 5 kV for signal / control / data / telecom lines;

e) Immunity to surges:

Name of EMC Standard: IEC 61000-4-5 (2005) “Testing & Measurement techniques for Surge immunity test"

Limits:-

i) For mains power input ports : (a)1.0 kV peak open circuit voltage for line to ground coupling (b) 0.5 kV peak open circuit voltage for line to line coupling

ii) For telecom ports : (a) 0.5 kV peak open circuit voltage for line to ground (b) 0.5 KV peak open circuit voltage for line to line coupling.

f) Immunity to conducted disturbance induced by Radio frequency fields:

Name of EMC Standard: IEC 61000-4-6 (2003) with amendment 1 (2004) & amd. 2 (2006) "Testing & measurement techniques-Immunity to conducted disturbances induced by radio- frequency fields "

Limits:-

Under the test level 2 {3 V r.m.s.}in the frequency range 150 kHz-80 MHz for AC / DC lines and Signal /Control/telecom lines.

g) Immunity to voltage dips & short interruptions (applicable to only ac mains power input ports, if any):

Name of EMC Standard: *IEC 61000-4-11 (2004) "Testing & measurement techniques- voltage dips, short interruptions and voltage variations immunity tests"*

Limits:-

i) a voltage dip corresponding to a reduction of the supply voltage of 30% for 500ms(i.e. 70 % supply voltage for 500 ms)

ii) a voltage dip corresponding to a reduction of the supply voltage of 60% for 200ms; (i.e. 40% supply voltage for 200ms) and

iii) a voltage interruption corresponding to a reduction of supply voltage of > 95% for 5s.

Note :- For checking compliance with the above EMC requirements, the method of measurements shall be in accordance with TEC Standard No. TEC/EMI/TEL-001/01/FEB-09 and the references mentioned therein unless otherwise specified specifically. Alternatively, corresponding relevant Euro Norms of the above IEC/CISPR standards are also acceptable subject to the condition that frequency range and test level are met as per above mentioned sub clauses (a) to (g) and TEC Standard No. TEC/EMI/TEL-001/01/FEB-09 The details of IEC/CISPR and their corresponding Euro Norms are as follows:

IEC/CISPR	**Euro Norm**
CISPR 11	EN 55011
CISPR 22	EN 55022
IEC 61000-4-2	EN 61000-4-2
IEC 61000-4-3	EN 61000-4-3
IEC 61000-4-4	EN 61000-4-4
IEC 61000-4-5	EN 61000-4-5
IEC 61000-4-6	EN 61000-4-6
IEC 61000-4-11	EN 61000-4-11

CHAPTER 7

SAFETY REQUIREMENTS

7.1Safety Requirements

The equipment shall conform to IS 13252 {2003} " Information Technology Equipment-safety: General requirement" [equivalent to IEC publication 60950-1]

CHAPTER 8

SECURITY REQUIREMENTS

Security Management

8.1 IMS Security

8.1.1 This section outlines the requirement for security. This section is divided to the following sub-areas:

8.1.2 **Access Domain Security** providing secure end-user access to the system and its services.

8.1.3 **Network Domain Security** covering network/site perimeter protection and communication protection between dispersed sites and between the systems the system and other (IP multimedia) networks according to the ETSI TS 133210. It also covers the site internal communication protection, node hardening and audit logging.

8.2 Access Domain Security

8.2.1 Access domain security covers application layer security for SIP and HTTP signaling between the User Agents (UA) and the system.

8.3 Network Domain Security

8.3.1 Inter-Domain Protection of Control Signaling

- Network domain security shall utilize Security Gateways (SEGs) for protecting the control signaling exchanged between the security domains or optionally within the security domain.

- Firewall shall be used to implement the SEG functionality in the system. SEGs shall employ IPsec (IP Security) for the protection of SIP signaling. The 3DES algorithm shall be used for encryption and HMAC-1 for integrity and authentication.

8.4 Site Security

8.4.1 Site security shall be organized according to the “defence in depth” principle constituting of:

- Perimeter protection

- Internal communication protection.

- Node protection

8.5 Site Perimeter Protection

Firewall shall be used for perimeter protection to mitigate general IP threats. Firewall filtering must be done based on various parameters, for example, port numbers, IP address, interfaces (for example, Untrusted, DMZ, Trusted) and transport protocols (TCP, UDP, SCTP). Ingress filtering should be used to check the source IP address to reduce the possibility of IP spoofing and Denial of Service (DoS) attacks.

8.6 Traffic Separation into Security Zones

Security zones must be implemented based on needed trust/security level for the concerned date. The traffic belonging to a specific security zone must be isolated from the traffic of other security zones.

- The traffic separation for the security zones shall be achieved with different types of Virtual Private Networks (VPNs).
- Within the IP backbone, VPNs shall be based on MPLS (Multi-protocol Label Switching). Traffic separation within the site is provided with the physical port based VLAN. Also the site L2/L3 switches and firewalls support traffic separation based on VLANs.
- Traffic separation for the accounting traffic (using RADIUS) must be done using dedicated interfaces. The traffic separation for CSCF and USPF nodes must be based on dedicated physical interfaces (ports) and dedicated Virtual IP (VIP) addresses.
- IPsec must be used as an overlay VPN for security sensitive data, independently from the other VPN techniques. For O&M and charging data IPsec ESP tunneling between SEGs must be used, when this data is transferred between sites.
- Firewall pairs shall be used guard the boundaries of each security zone.

8.7 Physical Access Protection

The physical access to nodes must be protected for unauthorized access.

8.8 O&M Security covering management access to the nodes and the protection of O&M, according and provisioning traffic

The O&M traffic is very critical for a system and in the IMS system the network elements shall have the possibility to be configured with separate interfaces for he O&M traffic. Other O&M security function that should be supported are:

- User access authorization based on username and password shall be supported.
- The O&M traffic shall protected by encrypted connections, SSH, SSL and DES for the various protocols.

8.9 Lawful Interception

The Lawful Interception and emergency service support shall be as per applicable TEC GR or latest in force.

8.10 Operator security functions: O & M operators can be granted limited access to the resources with user login and password security functions. All O & M administrative activities shall be controlled by a unified and consistent authentication and authorisation control system that provides for secure mechanisms to admit or prevent the execution of O & M tasks.

8.10.1 In case of outages of the offered O & M solution or the underlying IP infrastructure the O & M platform shall be able to perform automated resynchronisation such that no alarms, no performance data and no changes to configuration made are lost.

8.10.2 Support of System Maintenance including cold start, daily operations, software maintenance, software upgrade and hardware maintenance functions shall be available.

8.10.3 In case of hardware failure, it shall be able to isolate the failed hardware and automatically switch over to backup hardware to ensure the normal operation of the system. In case of software failure, system shall provide some self-correction and automatic recovery capability including reboot and reload etc.

8.10.4 When Hardware/Software failure degrades QoS, system shall continue operation. Redundancy shall be offered to critical components in the system to ensure automatic isolation and switchover or system reconfiguration in case of failure.

8.10.5 The system shall record various faults along with time stamps. It shall be possible to retrieve the fault log through man-machine command/GUI based command.

8.10.6 The system should detect the devices which are blocked and should record the number of times it is blocked with its identity if it exceeds the threshold value. In such cases, It should also generate alarm.

CHAPTER 9

OTHER MANDATORY REQUIREMENTS

9.1 Operation and Maintenance (O&M)

9.1.1 O & M functions: Atleast, but not limited to the following O&M functions shall be provided.

9.1.2 It shall be possible to integrate the O & M of the IMS nodes with the Operational & Maintenance Centre (OMC) for the existing PSTN. All the necessary software/hardware upgrade required to achieve the integration shall form the part of the IMS.

9.1.3 The OMC platform shall be used to manage all the IMS nodes including core and support functions (DNS/ ENUM or provisioning system etc.).

9.1.4 System shall be designed for easy software and hardware upgrade. The updated or modified software /hardware shall be compatible with other existing software/hardware.

9.1.5 Logging: The dialogue between the OMC and network elements shall be logged so that, in case of error, the work procedures can be understood and any problem that occurred can be analysed. The log shall include operation time, operation contents etc.

9.2 Routine/ Diagnostic Tests

9.2.1 Provision shall exist for routine tests of the supplied system either automatically or manually through man-machine command.

9.2.2 There shall be provision for diagnostic testing to know the health of each module in the system like running normal or not, communication link available or not etc.

9.3 Requirements Specific Millennium Problem

The equipment hardware and software shall not pose any problem, due to changes in data time caused by events such as changeover of millennium/ century, leap year etc., in the normal functioning.

9.4 Alarm messages shall contain but not limited to, the following :

i) date

ii) time

iii) severity

iv) unique identifying number

v) user defined component identifier

vi) user defined category

vii) alarm text

viii) Component/ node/ interface

ix) detailed alarm description including probable cause and impact.

x) Possible ways to rectify the alarm.

9.4.1 The system shall provide tools to enable tracing, fault isolation and fault diagnosis in both the signalling and bearer planes as well as on system, application and service level in order to perform “Route Cause Analysis”.

9.4.2 The Fault Management System shall comprise an interface to the Performance Management System in order to allow for alarming and clearing of performance degradation.

9.4.3 The Fault Management System shall comprise a 'Maintenance Function' that allows for suppressing alarms for IMS components that are temporarily out of order e. g. due to upgrade installations, maintenance task etc.

9.5 Availability / Redundancy /MTBF

9.5.1 The IMS nodes viz. CSCF (P-CSCF, S-CSCF, I-CSCF), MRF (MRFC, MRFP), BGCF, IMS-ALG, and other servers shall have availability of 99,999% and suitable redundancy shall be provided to achive the same.

9.5.2 The hardware and software failures as well as software upgrades of a single module in any of the IMS nodes shall not cause total system failure and shall not affect established sessions.

9.5.3 The system shall have MTBF values of at least 10,000 hours for the single nodes and for a complete system in the minimum configuration (P-CSCF, S-CSCF, I-CSCF, BGCF, MRF etc.)

9.5.4 The system shall support geographical redundancy.

9.6 System Reliability

The IMS nodes shall be designed for non-stop operation, and the platform shall incorporate duplicated hardware and software modularity, which enables individual modules to be upgraded without disturbing traffic.

9.7 Overload Control

9.7.1 This function allows the system to take care of possible overload conditions. The system shall have adequate buffering capacity to take care of temporary overload conditions in the network. The network shall silently discard the

packets in case of overload to avoid a network outage arising from overload situations. It shall be possible to reject new activations during overload conditions. Suitable alarms shall be generated to indicate overload condition.

9.7.2 There shall be an automatic mechanism for rejecting new sessions when overload conditions are met. All IMS applications shall have traffic limitation based on the platform function overload control. When the traffic crosses a configurable threshold for processor or memory load, the application shall refuse all new requests for calls, while the existing calls are served as normal. When a session request is received, the processor load level is checked. If there is an overload situation, the request shall be rejected.

9.7.3 The following procedures, to avoid overload condition in all equipment processors, shall be described:

i) Overload control procedures

ii) Threshold of triggering overload control

9.7.4 The impact on traffic and system performance, when overload control is triggered, shall be minimum for on-going traffic. CSCF shall discard the new request.

9.7.5 It shall be possible to combine physical interface when using a combined CSCF.

9.8 Traffic measurement

9.8.1 It shall be possible to record all traffic related information passing through the concerned node, such as number of packet attempt, number of packet routed, total data volume, QoS wise traffic, mean throughput, congestion and utilisation of each interface, processor load, memory usage and hard disk usage.

9.8.2 By using the above parameters, it shall be possible, through customisation, to generate reports in any format as per the requirement of service provider.

9.8.3 It shall also be possible to record the traffic hourly, daily, weekly, fortnightly, monthly or during any interval as specified by service provider.

9.9 Synchronisation

The system shall be capable of synchronising with NTP server.

CHAPTER - 10

Desirable requirements(operator specific)

10.1 Note:. For procurement purposes, Purchaser shall specify the requirements in respect of different clauses including, but not limited to the following:

1. Various dimensioning parameters e.g. traffic handling capacity, storage type and volume, synchronous or asynchronous etc. shall be indicated.

2. The software related licenses for the support of all protocols and interfaces mentioned in this GR shall be ensured.

3. Qualitative Requirements (QR): The purchase shall specify quality standards like ISO 9002 or ISO 9001: 2000 certification.

4. The manufacturer shall furnish the MTBF value. The calculations of MTBF shall be based on the guidelines given in tendering

5. Environment Conditions: The purchaser shall specify the requirements of Environment Conditions that the system will satisfy as specified in Quality Measure Manual for relevant category of equipment.

6. Number of copies (hard and soft) of following documents required shall be specified by the purchaser.

   i). System description documents

   ii). System operation and maintenance documents

   iii). Training documents

   iv). Installation Documents

   v). Repair related documents

   Further details of documentation required have to be specified by the purchaser.

10.2 The purchaser shall specify the time frame for the requirement of three stages of IMS support viz. Release 5, Release-6, Release-7.

.

10.3 The purchaser shall specify the protocols for transport & signalling layer specifically at various interfaces at the time of procurement depending on the requirement and availability of the commercially proven equipment from multiple vendors..

10.4 The purchaser may specify the actual requirements for lawful interception and monitoring like number of subscribers to be monitored, number of monitoring agencies etc. as per latest instructions from licensor/LEAs

10.5 **Interfaces:** The purchaser shall specify the types of interfaces, number of interfaces and ports as per requirements of different interfaces.

10.6 **System capacity:** The purchaser shall review and specify the capacity & performance parameters as per the requirements depending on number of subscribers to start with, maximum expansion envisaged, type of call/ traffic model etc. It shall give details of the call profile/ traffic model for which this capacity & performance shall be supported.

10.7 The I-CSCF shall have capability to generate and transfer CDRs (optional to be decided by tendering authority)

10.8 The purchaser shall indicate the maintenance updates and updates for new services and features required in future along with commercial terms and conditions for the same.

10.9 The purchaser shall specify various IMS applications/ services that will be supported by the IMS core network.

10.10 Accounting information generation (optional to be decided by tendering authority)

10.11 The purchaser shall specify the number of ports for server using G. 711 codec.

10.12 Field Proveness and Interoperability: The tendering authority may specify the requirement of equipment being deployed in multiple countries and networks & their period of deployment. This may be mentioned as, “The equipment shall have been field deployed commercially across multiple countries and network & for a reasonable period of time of at least six months”. Tendering authority may also specify the various technologies / vendors of Circuit Switched Core Network (CS-CN) and associated sub-systems with which IMS system has to inter-operate.

MGCF shall comply with the following standards released

10.13 The MGCF shall support the functionality of AGCF(Access gateway control function

MGCF shall comply with the following standards released

- DES-02029-NGN-R1 Core IMS Architecture
- DES -02032-NGN-R1 Charging)

- DTS-03022-NGN-R1 NGN Call Diversion (CDiv)/call forwarding
- DES-03040- NGN-R1 Trunking Gateway Control Protocol stage2
- DES-03047-NGN-R1 Common Basic Communication procedures
- DTS-03054-NGN-R1 Common Basic Communication Procedure
- DTS-03069-NGN-R1 NGN Hold correction /alignment
- DES/TISPAN-03053-NGN-R1

10.14 IMS Dimensioning

The purchaser may specify the following interfaces as per requirement.

S. NO.	Items	Quantities
1. 1	a1 links	As per requirement
2.	a2 links	As per requirement
3.	a3 links	As per requirement
4.	a4 links	As per requirement
5.	Ia, links	As per requirement
6.	Cx, links	As per requirement
7.	Dh links	As per requirement
8.	Dx links	As per requirement
9.	e1 links	As per requirement
10.	e2 links	As per requirement
11.	e3 links	As per requirement
12.	e4 links	As per requirement
13.	Gm links	As per requirement
14.	Gq' links	As per requirement
15.	ISC links	As per requirement
16.	Ic links	As per requirement
17.	Ib links	As per requirement
18.	Ie links	As per requirement
19.	Iw links	As per requirement
20.	Mn links	As per requirement
21.	Mp links	As per requirement
22.	Mg links	As per requirement
23.	Mi links	As per requirement
24.	Mj links	As per requirement

25.	Mk links	As per requirement
26.	Mr links	As per requirement
27.	Mw links	As per requirement
28.	P1links	As per requirement
29.	Re links	As per requirement
30.	Rq links	As per requirement
31.	Sh links	As per requirement
32.	t1links	As per requirement
33.	t2 links	As per requirement
34.	t3 links	As per requirement
35.	Ut links	As per requirement
36.	z links	As per requirement

10.13 Power Supply

For all IMS nodes

.

Option 1:

The nodes shall be capable of working with –40 V to –57 V. D .C. input from power supply.

Switching mode Power Supply (SMPS) and VRLA battery to be used shall be as per TEC Generic Requirements No. GR/SMP –01 and GR/BAT-01 Respectively. Power supply and battery shall be modular and expendable to support the ultimate equipment configuration.

Option 2:

AC Mains supply of 220 Volts with a tolerance of -15% to + 10% would be available. The frequency may be 50 Hz $\pm$ 2 Hz. UPS and other power requirements are to be specified by the system developer. Relevant TEC Specification/ Generic Requirements as applicable may be referred

Purchase may specify the power requirement as per option1 or 2.

10.14 Additional Guidelines

10.14.1 In case a single CSCF node is not capable of meeting the requirements than multiple CSCF nodes shall be provided.

10.14.2 Signalling gateway can be integrated with MGCF or standalone.

10.14.3 The BGCF and S-CSCF shall be standalone or co-located .

10.14.4 BGCF shall have capability to generate and transfer CDRs and CDRs shall comply TISPAN DES-02029-NGN–R1

10.14.5 The capacity of the CSCF node shall be enough to support the following for a given number of the subscribers:

i) Number of simultaneously attached subscribers.

ii) The total throughput of the node.

iii) The design shall include adequate hardware redundancies so that failure of any single card or shelf controller component shall not result in denial of service to a group of subscribers.

iv) The above shall be applicable for designing the links between the various nodes carrying either the signalling information or the user data.

v) Signal domain should support minimum of 500000 users.

vi) Dimensioning parameter of others nodes are given below

P-CSCF: 500,000 SEBH

S-CSCF: 500, 000 SEBH

I-CSCF: 500, 000 SEBH

USPF: 750,000 Subs

A-SBC / SBG: 15 K sessions

N-SBG : 15 K sessions

Glossary

2G	2nd Generation
3G	3rd Generation
4G	4th Generation
3GPP	3rd Generation Partnership Project
AA	Anonymous Access
AF	Application Function
AAL	ATM Adaptation Layer
ACL	Access Control List
AMR	Adaptive Multi-Rate
AOR	Address of Record
API	Application Program Interface
APN	Access Point Name
ARP	Address Resolution Protocol
A-RACF	Access -Resource and Admission Control
AS	Application Server
ASCII	American Standard Code for Information Interchange
ASN	Abstract Syntax Notation
ATM	Asynchronous Transfer Mode
AuC	Authentication Centre
AUTN	Authentication Token
BG	Border Gateway
BGF	Border Gateway Function
BGCF	Breakout Gateway Control Function
BGP	Border Gateway Protocol
BS	Bearer Service
BSNL	Bharat Sanchar Nigam Limited
CAC	Connection Admission Control
CAMEL	Customised Applications for Mobile network Enhanced Logic
CAP	CAMEL Application Part
C-BGF	Core- Border Gateway Function
CCF	Call Control Function
CDMA	Code Division Multiple Access
CDR	Charging Detail Record
CD-ROM	Compact Disk-Read Only Memory
CFNRc	Call Forwarding Not Reachable
CFU	Call Forwarding Unconditional
CG	Charging Gateway
CGF	Charging Gateway Function
CLI	Calling Line Identification
CLF	Connectivity Session Location and Repository Function
CM	Configuration Management
CMT	Centralised Maintenance Terminal
CN	Core Network
CoS	Class of Service
CPU	Central Processing Unit
CRI	Call Related Information

CS	Circuit Switched
P-CSCF	Proxy-Call Session Control Function-
I-CSCF	Integrity-Call Session Control Function
S-CSCF	Serving-Call Session Control Function
CSD	Circuit Switched Data
CSE	CAMEL Service Environment
CUG	Close User Group
DCCA	Diameter Credit Control Application
DD	Delivery Domain
DiffServ	Differentiated Services
DHCP	Dynamic Host Configuration Protocol
DNIC	Data Network Identification Code
DNS	Domain Name Server
DPC	Destination Point Code
DSCP	DiffServ Code Point
EMI	Electro Magnetic Interference
ENUM	E.164 Number
ETSI	European Telecommunication Standard Institute
FC	Flow Control
FDDI	Full Duplex Digital Interface
FDX	Full Duplex
FM	Fault and event Management
FMC	Fixed Mobile Convergence
FTAM	File Transfer Access Management
FTP	File Transfer Protocol
G-CDR	GGSN-CDR
GEA	GPRS Encryption Algorithm
GERAN	GPRS EDGE Radio Access Network
GGSN	Gateway GPRS Support Node
GMLC	Gateway MLC
GMM/SM	GPRS Mobility Management / Session Management
GMSC	Gateway MSC
GUP	Generic User Profile
HDX	Half Duplex
HPLMN	Home Public Land Mobile Network
HSS	Home Subscriber Server
IBCF	Interconnection Border Control Function
IBGF	Interconnect Border Gateway Function
ICMP	Internet Control Message Protocol
I-CSCF	Interrogating-CSCF
IETF	Internet Engineering Task Force
IK	Integrity Key
IM	IP Multimedia
IMEI	International Mobile Equipment Identity
IMPCS	India Mobile Personal Communication System
IMPI	IMS Private Indentity
IMS	IP Multimedia Subsystem
IMS ALG	IMS Application Level Gateway
IN	Intelligent Network

IP	Internet Protocol
IP-CAN	IP-Connectivity Access Network
IPSec	Internet Protocol Security
IPv4/IPv6	Internet Protocol version-4/ Internet Protocol version-6
ISDN	Integrated Service Digital Network
ISUP	ISDN User Part
ITU	International Telecommunication Union
IWF	Interworking Function
LMT	Local Maintenance Terminal
LPC	Local Point Code
MAC	Medium Access Control
MRF	Media Resource Function
MGCF	Media Gateway Control Function
MGF	Media Gateway Function
MHz	Mega Hertz
MMD	Multi Media Domain
MPLS	Multi Protocol Label Switching
MTBF	Mean Time Between Failure
MTTR	Mean Time To Restore
NAAS	Network Attached Sub- Subsystem
NEBS	Network Equipment Building System
NP	Network Performance
NS	Network Service
NSAPI	Network layer Service Access Point Identifier
NSS	Network Switching Sub-system
O&M	Operation & Maintenance
OMC	Operation & Maintenance Centre
OS	Operating System
OSA	Open Services Architecture
OSPF	Open Shortest Path First
PC	Personal Computer, Packet Core, Point Code
P-CSCF	Proxy-CSCF
PCB	Printed Circuit Board
PCU	Packet Control Unit
PDCH	Packet Data Channel
PDF	Policy Decision Function
PDN	Packet Data Network
PDP	Packet Data Protocol (e.g., IP or X.25)
PDU	Protocol Data Unit
PHB	Per-Hop Behavior
PLMN	Public Land Mobile Network
PM	Performance Management
PNNI	Private Network-to-Network Interface
PoI	Point of Interconnect
PPP	Point-to-Point Protocol
PPS	Packets Per Second
PSPDN	Packet Switched Packet Data Network
PSTN	Public Switched Telephone Network
PTP	Point To Point

PVC	Permanent Virtual Circuit
QoS	Quality of Service
RADIUS	Remote Authentication Dial-In User Service
RAI	Routing Area Identity
RANAP	Radio Access Network Application Part
RAU	Routing Area Update
RCEF	Resource Control Enforcement Function
RF	Radio Frequency
RFC	Request for Comments
RIP	Routing Information Protocol
RLC	Radio Link Control
RNS	Radio Network System
RRM	Radio Resource Management
SAAL	Signalling ATM Adaptation Layer
S-CDR	SGSN - CDR
SCF	Service Control Function
SCP	Service Control Point
S-CSCF	Serving-CSCF
SCS	Service Capability Server
SDP	Session Description Protocol
SEG	Security Gateway
SEBH	Session Busy Hour
SCTP	Stream Control Transport Protocol
SGW	Signalling Gateway
SIGTRAN	Signalling Transport
SPDF	Session Based Policy Decision Function
SIM	Subscriber Identity Module
SIP	Session Initiation Protocol
SLF	Subscription Locator Function
SNMP	Simple Network Management Protocol
SNDC	Sub-Network Dependent Convergence
SNDCP	Sub-Network Dependent Convergence Protocol
SRF	Specialised Resource Function
SRNC	Serving Radio Network Controller
SRNS	Serving Radio Network System
SSCF-NNI	Service Specific Coordination Function – Network Node Interface
SSCOP	Service Specific Connection Oriented Protocol
SSF	Service Switching Function
SS7	Signalling System #7
STP	Signalling Transfer Point
SVC	Switched Virtual Circuit
TCAP	Transaction Capabilities Application Part
TCP	Transmission Control Protocol
TDMA	Time Division Multiple Access
TE	Terminal Equipment
TEC	Telecommunication Engineering Centre
THIG	Topology Hiding Inter-network Gateway
TID	Tunnel Identifier

TISPAN	Telecommunication and Internet Converged Services and Protocol for Advanced Network
ToS	Type of Service
TRAU	Transcoder and Rate Adaptor Unit
TrGW	Transition Gateway
UDP	User Datagram Protocol
UE	User Equipment
UNI	User-to-Network Interface
UP	User Plane
UPC	Usage Parameter Control
URL	Universal Resource Locator
USPF	/UPSFUniversal Subscriber Profile Function/User Profile Server Function

----------End of the Document----------