International Telecommunication Union

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

Y.2201

(09/2009)

SERIES Y: GLOBAL INFORMATION INFRASTRUCTURE, INTERNET PROTOCOL ASPECTS AND NEXT-GENERATION NETWORKS

Next Generation Networks – Service aspects: Service capabilities and service architecture

Requirements and capabilities for ITU-T NGN

Recommendation ITU-T Y.2201

ITU-T Y-SERIES RECOMMENDATIONS

GLOBAL INFORMATION INFRASTRUCTURE, INTERNET PROTOCOL ASPECTS AND NEXT-GENERATION NETWORKS

GLOBAL INFORMATION INFRASTRUCTURE	
General	Y.100–Y.199
Services, applications and middleware	Y.200–Y.299
Network aspects	Y.300–Y.399
Interfaces and protocols	Y.400–Y.499
Numbering, addressing and naming	Y.500–Y.599
Operation, administration and maintenance	Y.600–Y.699
Security	Y.700–Y.799
Performances	Y.800–Y.899
INTERNET PROTOCOL ASPECTS	
General	Y.1000–Y.1099
Services and applications	Y.1100–Y.1199
Architecture, access, network capabilities and resource management	Y.1200–Y.1299
Transport	Y.1300–Y.1399
Interworking	Y.1400–Y.1499
Quality of service and network performance	Y.1500–Y.1599
Signalling	Y.1600–Y.1699
Operation, administration and maintenance	Y.1700–Y.1799
Charging	Y.1800–Y.1899
IPTV over NGN	Y.1900–Y.1999
NEXT GENERATION NETWORKS	
Frameworks and functional architecture models	Y.2000–Y.2099
Quality of Service and performance	Y.2100–Y.2199
Service aspects: Service capabilities and service architecture	**Y.2200–Y.2249**
Service aspects: Interoperability of services and networks in NGN	Y.2250–Y.2299
Numbering, naming and addressing	Y.2300–Y.2399
Network management	Y.2400–Y.2499
Network control architectures and protocols	Y.2500–Y.2599
Future networks	Y.2600–Y.2699
Security	Y.2700–Y.2799
Generalized mobility	Y.2800–Y.2899
Carrier grade open environment	Y.2900–Y.2999

For further details, please refer to the list of ITU-T Recommendations.

Recommendation ITU-T Y.2201

Requirements and capabilities for ITU-T NGN

Summary

Recommendation ITU-T Y.2201 provides high-level requirements for services and capabilities of a next generation network (NGN).

Source

Recommendation ITU-T Y.2201 was approved on 12 September 2009 by ITU-T Study Group 13 (2009-2012) under the WTSA Resolution 1 procedure. This edition includes Corrigendum 1 which was approved on 29 January 2010 by ITU-T Study Group 13.

Keywords

Accounting, addressing, authentication, authorization, capabilities, capability requirements, charging, context awareness, enterprise network, identification, identity management, interoperability, interworking, IPTV, IPv6 support, management, mobility, multicast, naming, NGN, numbering, OAM, open service environment, policy, privacy, profile, QoS, security, service enabler.

FOREWORD

The International Telecommunication Union (ITU) is the United Nations specialized agency in the field of telecommunications, information and communication technologies (ICTs). The ITU Telecommunication Standardization Sector (ITU-T) is a permanent organ of ITU. ITU-T is responsible for studying technical, operating and tariff questions and issuing Recommendations on them with a view to standardizing telecommunications on a worldwide basis.

The World Telecommunication Standardization Assembly (WTSA), which meets every four years, establishes the topics for study by the ITU-T study groups which, in turn, produce Recommendations on these topics.

The approval of ITU-T Recommendations is covered by the procedure laid down in WTSA Resolution 1.

In some areas of information technology which fall within ITU-T's purview, the necessary standards are prepared on a collaborative basis with ISO and IEC.

NOTE

In this Recommendation, the expression "Administration" is used for conciseness to indicate both a telecommunication administration and a recognized operating agency.

Compliance with this Recommendation is voluntary. However, the Recommendation may contain certain mandatory provisions (to ensure e.g., interoperability or applicability) and compliance with the Recommendation is achieved when all of these mandatory provisions are met. The words "shall" or some other obligatory language such as "must" and the negative equivalents are used to express requirements. The use of such words does not suggest that compliance with the Recommendation is required of any party.

INTELLECTUAL PROPERTY RIGHTS

ITU draws attention to the possibility that the practice or implementation of this Recommendation may involve the use of a claimed Intellectual Property Right. ITU takes no position concerning the evidence, validity or applicability of claimed Intellectual Property Rights, whether asserted by ITU members or others outside of the Recommendation development process.

As of the date of approval of this Recommendation, ITU had not received notice of intellectual property, protected by patents, which may be required to implement this Recommendation. However, implementers are cautioned that this may not represent the latest information and are therefore strongly urged to consult the TSB patent database at http://www.itu.int/ITU-T/ipr/.

CONTENTS

Recommendation ITU-T Y.2201

Requirements and capabilities for ITU-T NGN

1 Scope

This Recommendation specifies the high-level requirements for the development of a set of ITU-T Recommendations which will constitute NGN.

The high-level requirements and related capabilities specified in this Recommendation are aligned with the general goals and objectives captured in [ITU-T Y.2001] and are based on the objectives of NGN release 2 [b-ITU-T Y.Sup-7].

The requirements are mainly provided from a high-level perspective, and are not intended to constitute precise functional requirements for the different NGN entities.

More detailed requirements are outside the scope of this Recommendation.

It is recognized that a specific realization of NGN may be constituted by an arbitrary set (or superset) of services supported in NGN and of capabilities as specified in this Recommendation.

NOTE 1 – Text taken from [ITU-T Y.2201] uses blue font. Also, Appendix I identifies the main differences in terms of high-level requirements and capabilities between this Recommendation and [ITU-T Y.2201].

NOTE 2 – It is also required to consider how NGN can contribute to energy savings. However, studies for this topic are ongoing in ITU-T Study Group 5 based on the output from the ITU-T Focus Group on ICTs and Climate Change. So requirements from energy savings aspects are for further study in this Recommendation. For the output from the ITU-T Focus Group on ICTs and Climate Change, please see [b-ITU-T Climate].

2 References

The following ITU-T Recommendations and other references contain provisions which, through reference in this text, constitute provisions of this Recommendation. At the time of publication, the editions indicated were valid. All Recommendations and other references are subject to revision; users of this Recommendation are therefore encouraged to investigate the possibility of applying the most recent edition of the Recommendations and other references listed below. A list of the currently valid ITU-T Recommendations is regularly published. The reference to a document within this Recommendation does not give it, as a stand-alone document, the status of a Recommendation.

[ITU-T E.106] Recommendation ITU-T E.106 (2003), *International Emergency Preference Scheme (IEPS) for disaster relief operations*.

[ITU-T E.107] Recommendation ITU-T E.107 (2007), *Emergency Telecommunications Service (ETS) and interconnection framework for national implementations of ETS*.

[ITU-T E.164] Recommendation ITU-T E.164 (2005), *The international public telecommunication numbering plan*.

[ITU-T E.212] Recommendation ITU-T E.212 (2008), *The international identification plan for public networks and subscriptions*.

[ITU-T G.711] Recommendation ITU-T G.711 (1988), *Pulse code modulation (PCM) of voice frequencies*.

[ITU-T G.722] Recommendation ITU-T G.722 (1988), *7 kHz audio-coding within 64 kbit/s*.

[ITU-T G.722.2] Recommendation ITU-T G.722.2 (2003), *Wideband coding of speech at around 16 kbit/s using Adaptive Multi-Rate Wideband (AMR-WB)*.

[ITU-T G.729] Recommendation ITU-T G.729 (2007), *Coding of speech at 8 kbit/s using conjugate-structure algebraic-code-excited linear prediction (CS-ACELP)*.

[ITU-T G.729.1] Recommendation ITU-T G.729.1 (2006), *G.729-based embedded variable bit-rate coder: An 8-32 kbit/s scalable wideband coder bitstream interoperable with G.729*.

[ITU-T G.808.1] Recommendation ITU-T G.808.1 (2006), *Generic protection switching – Linear trail and subnetwork protection*.

[ITU-T H.263] Recommendation ITU-T H.263 (2005), *Video coding for low bit rate communication*.

[ITU-T H.264] Recommendation ITU-T H.264 (2005), *Advanced video coding for generic audiovisual services*.

[ITU-T I.610] Recommendation ITU-T I.610 (1999), *B-ISDN operation and maintenance principles and functions*.

[ITU-T M.3050.0] Recommendation ITU-T M.3050.0 (2007), *Enhanced Telecom Operations Map (eTOM) – Introduction*.

[ITU-T M.3050.1] Recommendation ITU-T M.3050.1 (2007), *Enhanced Telecom Operations Map (eTOM) – The business process framework*.

[ITU-T M.3060] Recommendation ITU-T M.3060/Y.2401 (2006), *Principles for the Management of Next Generation Networks*.

[ITU-T Q.825] Recommendation ITU-T Q.825 (1998), *Specification of TMN applications at the Q3 interface: Call detail recording*.

[ITU-T Q.1703] Recommendation ITU-T Q.1703 (2004), *Service and network capabilities framework of network aspects for systems beyond IMT-2000*.

[ITU-T Q.1706] Recommendation ITU-T Q.1706/Y.2801 (2006), *Mobility management requirements for NGN*.

[ITU-T X.462] Recommendation ITU-T X.462 (1996), *Information technology – Message Handling Systems (MHS) Management: Logging information*.

[ITU-T X.805] Recommendation ITU-T X.805 (2003), *Security architecture for systems providing end-to-end communications*.

[ITU-T Y.101] Recommendation ITU-T Y.101 (2000), *Global Information Infrastructure terminology: Terms and definitions*.

[ITU-T Y.110] Recommendation ITU-T Y.110 (1998), *Global Information Infrastructure principles and framework architecture*.

[ITU-T Y.1271] Recommendation ITU-T Y.1271 (2004), *Framework(s) on network requirements and capabilities to support emergency telecommunications over evolving circuit-switched and packet-switched networks*.

[ITU-T Y.1541] Recommendation ITU-T Y.1541 (2006), *Network performance objectives for IP-based services*.

[ITU-T Y.1710] Recommendation ITU-T Y.1710 (2002), *Requirements for Operation & Maintenance functionality in MPLS networks*.

[ITU-T Y.1730] Recommendation ITU-T Y.1730 (2004), *Requirements for OAM functions in Ethernet-based networks and Ethernet services*.

[ITU-T Y.1901] Recommendation ITU-T Y.1901 (2009), *Requirements for the support of IPTV services*.

[ITU-T Y.2001] Recommendation ITU-T Y.2001 (2004), *General overview of NGN*.

[ITU-T Y.2012] Recommendation ITU-T Y.2012 (2006), *Functional requirements and architecture of the NGN release 1*.

[ITU-T Y.2051] Recommendation ITU-T Y.2051 (2008), *General overview of IPv6-based NGN*.

[ITU-T Y.2091] Recommendation ITU-T Y.2091 (2008), *Terms and definitions for Next Generation Networks*.

[ITU-T Y.2111] Recommendation ITU-T Y.2111 (2008), *Resource and admission control functions in next generation networks*.

[ITU-T Y.2201] Recommendation ITU-T Y.2201 (2007), *NGN release 1 requirements*.

[ITU-T Y.2212] Recommendation ITU-T Y.2212 (2008), *Requirements of managed delivery services*.

[ITU-T Y.2213] Recommendation ITU-T Y.2213 (2008), *NGN service requirements and capabilities for network aspects of applications and services using tag-based identification*.

[ITU-T Y.2215] Recommendation ITU-T Y.2215 (2009), *Requirements and framework for the support of VPN services in NGN, including the mobile environment*.

[ITU-T Y.2233] Recommendation ITU-T Y.2233 (2008), *Requirements and framework allowing accounting and charging capabilities in NGN*.

[ITU-T Y.2234] Recommendation ITU-T Y.2234 (2008), *Open service environment capabilities for NGN*.

[ITU-T Y.2236] Recommendation ITU-T Y.2236 (2009), *Framework for NGN support of multicast-based services*.

[ITU-T Y.2701] Recommendation ITU-T Y.2701 (2007), *Security requirements for NGN release 1*.

[ITU-T Y.2720] Recommendation ITU-T Y.2720 (2009), *NGN identity management framework*.

[ITU-T Z.100] Recommendation ITU-T Z.100 (2007), *Specification and Description Language (SDL)*.

[ETSI TS 126.071] ETSI TS 26.071 V6.0.0 (2004-12), *Digital cellular telecommunications system (Phase 2+); Universal Mobile Telecommunications System (UMTS); AMR speech Codec; General description (3GPP TS 26.071 version 6.0.0 Release 6)*.

[TIA-127-C] TIA Standard TIA-127-C (2007), *Enhanced Variable Rate Codec, Speech Service Options 3, 68, and 70 for Wideband Spread Spectrum Digital Systems*.

3 Definitions

3.1 Terms defined elsewhere

This Recommendation uses the following terms defined elsewhere:

3.1.1 accounting [ITU-T X.462]: The action of collecting information on the operations performed within a system and the effects thereof.

3.1.2 address [ITU-T Y.2091]: An address is the identifier for a specific termination point and is used for routing to this termination point.

3.1.3 application network interface (ANI) [ITU-T Y.2012]: Interface which provides a channel for interactions and exchanges between applications and NGN elements. The ANI offers capabilities and resources needed for realization of applications.

3.1.4 billing [ITU-T Q.1703]: Administrative function to prepare bills to service customers, to prompt payments, to obtain revenues and to take care of customer reclaims.

3.1.5 charging [ITU-T Q.825]: The set of functions needed to determine the price assigned to the service utilization.

3.1.6 corporate network [ITU-T Y.2701]: A private network that supports multiple users and may be in multiple locations (e.g., an enterprise, campus).

NOTE – Equipment of the private network is owned by or managed on behalf of an enterprise, and is interconnected to provide telecommunication services to a defined group of users belonging to that enterprise.

3.17 customer [ITU-T M.3050.1]: The customer buys products and services from the enterprise or receives free offers or services. A customer may be a person or a business.

3.1.8 end user [ITU-T M.3050.1]: The end user is the actual user of the products or services offered by the enterprise. The end user consumes the product or service. See also the definition of subscriber.

3.1.9 entity [ITU-T Y.2720]: Anything that has separate and distinct existence that can be uniquely identified. In the context of IdM, examples of entities include subscribers, users, network elements, networks, software applications, services and devices. An entity may have multiple identifiers.

3.1.10 federation [ITU-T Y.2720]: Establishing a relationship between two or more entities or an association comprising any number of service providers and identity providers.

3.1.11 handover [ITU-T Q.1706]: The ability to provide services with some impact on their service level agreements to a moving object during and after movement.

3.1.12 home network [ITU-T Q.1706]: The network to which a mobile user is normally connected, or the service provider with which the mobile user is associated, and where the user's subscription information is managed.

3.1.13 identifier [ITU-T Y.2091]: An identifier is a series of digits, characters and symbols or any other form of data used to identify subscriber(s), user(s), network element(s), function(s), network entity(ies) providing services/applications, or other entities (e.g., physical or logical objects). Identifiers can be used for registration or authorization. They can be either public to all networks, shared between a limited number of networks or private to a specific network (private IDs are normally not disclosed to third parties).

3.1.14 identity [ITU-T Y.2720]: Information about an entity that is sufficient to identify that entity in a particular context.

3.1.15 identity management [ITU-T Y.2720]: Set of functions and capabilities (e.g., administration, management and maintenance, discovery, communication exchanges, correlation and binding, policy enforcement, authentication and assertions) used for:

– assurance of identity information (e.g., identifiers, credentials, attributes);

– assurance of the identity of an entity (e.g., users/subscribers, groups, user devices, organizations, network and service providers, network elements and objects, and virtual objects); and

– enabling business and security applications.

3.1.16 identity provider [ITU-T Y.2720]: An entity that creates, maintains and manages trusted identity information of other entities (e.g., user/subscribers, organizations, and devices) and offers identity-based services based on trust, business and other types of relationship.

3.1.17 Internet [ITU-T Y.101]: A collection of interconnected networks using the Internet Protocol which allows them to function as a single, large virtual network.

3.1.18 IPv6-based NGN [ITU-T Y.2051]: This refers to NGN that supports addressing, routing protocols, and services associated with IPv6. An IPv6-based NGN shall recognize and process the IPv6 headers and options, operating over various underlying transport technologies in the transport stratum.

3.1.19 mobility [ITU-T Y.2001]: The ability for the user or other mobile entities to communicate and access services irrespective of changes of the location or technical environment. The degree of service availability may depend on several factors including the Access Network capabilities, service level agreements between the user's home network and the visited network (if applicable), etc. Mobility includes the ability of telecommunication with or without service continuity.

NOTE – In [ITU-T Y.2001] this is called "generalized mobility".

3.1.20 mobility management [ITU-T Q.1706]: The set of functions used to provide mobility. These functions include authentication, authorization, location updating, paging, download of user information and more.

3.1.21 nomadism [ITU-T Q.1706]: The ability of the user to change their network access point on moving. When changing the network access point, the user's service session is completely stopped and then started again, i.e., there is no service continuity or hand-over used. It is assumed that normal usage pattern is that users shut down their service session before attaching to a different access point.

3.1.22 personally identifiable information [ITU-T Y.2720]: The information pertaining to any living person, which makes it possible to identify such individual (including the information capable of identifying a person when combined with other information even if the information does not clearly identify the person).

3.1.23 personal mobility [ITU-T Q.1706]: This is the mobility for those scenarios where the user changes the terminal used for network access at different locations. The ability of a user to access telecommunication services at any terminal on the basis of a personal identifier, and the capability of the network to provide those services delineated in the user's service profile.

3.1.24 presence [ITU-T Y.2720]: A set of attributes that characterizes an entity relating to current status.

3.1.25 public network [b-ITU-T I.570]: A network which provides services to the general public.

NOTE – This definition does not include legal or regulatory aspects and does not indicate any aspect of ownership.

3.1.26 **roaming** [ITU-T Q.1706]: This is the ability of users to access services according to their user profile while moving outside of their subscribed home network, i.e., by using an access point of a visited network. This requires the capability for access to the visited network, the existence of an interface between home network and visited network, as well as a roaming agreement between the respective network operators.

3.1.27 **seamless handover** [ITU-T Q.1706]: It is a special case of mobility with service continuity since it preserves the ability to provide services without any impact on their service level agreements to a moving object during and after movement.

3.1.28 **service** (Supplement 1 to Z-series Recommendations): A set of functions and facilities offered to a user by a provider.

3.1.29 **service continuity** [ITU-T Q.1706]: The ability for a moving object to maintain ongoing service over including current states, such as user's network environment and session for a service.

3.1.30 **subscriber** [ITU-T M.3050.1]: The subscriber is responsible for concluding contracts for the services subscribed to and for paying for these services.

3.1.31 **terminal mobility** [ITU-T Q.1706]: This is the mobility for those scenarios where the same terminal equipment is moving or is used at different locations. The ability of a terminal to access telecommunication services from different locations and while in motion, and the capability of the network to identify and locate that terminal.

3.1.32 **user network** [ITU-T Y.2701]: A private network consisting of terminal equipment that may have multiple users.

3.1.33 **visited network** [ITU-T Q.1706]: The network outside a home network that provides service to a mobile user. This term is more business significant than geographically significant.

3.2 Terms defined in this Recommendation

This Recommendation defines the following terms:

3.2.1 **break-in**: A communication from a user of a public network to a user of an enterprise network.

3.2.2 **break-out**: A communication from a user of an enterprise network to a user of a public network.

3.2.3 **business trunking**: Connection of a next generation corporate network (NGCN) to an NGN.

3.2.4 **business trunking application**: NGN application that either provides transit capabilities between next generation corporate networks (NGCNs), or break-in capabilities from NGN to NGCN and/or break-out capabilities from NGCN to NGN.

NOTE – A business trunking application may also provide additional services beyond basic break-in, break-out and transit capabilities to the NGCN.

3.2.5 **context awareness**: Context awareness is a capability to determine or influence a next action in telecommunication or process by referring to the status of relevant entities, which form a coherent environment as a context.

3.2.6 **corporate network user identifier**: Identifies a corporate network user on communications entering, leaving or transiting the NGN, either representing an originating corporate network user or as a globally routable target identity.

3.2.7 **enterprise communication**: Any communication that is either:

1) originated in a next generation corporate network (NGCN); or

2) terminated in an NGCN; or

3) originated in the NGN on behalf of an enterprise; or

4) terminated in the NGN on behalf of an enterprise;

and which is subject to special arrangements between the NGN operator and the enterprise.

3.2.8 enterprise communication capabilities: Any capability whether hosted in a next generation corporate network (NGCN) or an NGN that enables and/or enriches enterprise communications.

NOTE – Business trunking application, hosted enterprise services and virtual leased line are examples of enterprise communication capabilities hosted in NGN.

3.2.9 hosted enterprise services (HES): NGN application whereby the NGN hosts all originating and/or terminating business communication capabilities for enterprise users that are directly attached to NGN and have a subscription for this application in NGN.

NOTE – This is known commonly as IP-Centrex.

3.2.10 next generation corporate network (NGCN): Self-contained corporate network designed to take advantage of emerging IP-based communications solutions and that can have its own applications and service provisioning.

NOTE – For the purpose of this Recommendation, it is a corporate network that provides an IP-based interface to an NGN.

3.2.11 NGCN site: A separate part of a next generation corporate network (NGCN).

NOTE – An NGCN site might represent a part of an NGCN bound to a specific geographic location. When an NGCN site serves more than one geographic location, all locations served by that NGCN site would have access to an NGN concerned via the NGCN site's connectivity arrangement with that NGN. Communication between different NGCN sites belonging to the same NGCN can, but need not, pass through their respective NGN(s). For example, such communications might be routed by NGN(s) only during periods of high traffic or equipment outage within the NGCN. An NGCN site can have access to its NGN either directly or via some other NGN that provides a transit capability. An NGCN can have NGCN sites in different countries.

3.2.12 priority classification: Classification of traffic classes according to different levels of priorities.

3.2.13 priority enabling mechanisms: The mechanisms by which appropriate treatment of traffic according to priority classes may be enabled in the network.

3.2.14 private network traffic: Traffic sent to or received from an NGN for processing according to an agreed set of rules specific to an enterprise or a community of closely related enterprises.

3.2.15 public network traffic: Traffic sent to or received from an NGN for processing according to the normal NGN rules.

3.2.16 single sign-on: The ability to use an authentication assertion from one network operator/service provider to another operator/service provider for a user either accessing a service or roaming into a visited network.

3.2.17 terminal equipment identifier: A unique identifier of a terminal equipment.

3.2.18 user: A user includes end user [ITU-T Y.2091], person, subscriber, system, equipment, terminal (e.g., FAX, PC), (functional) entity, process, application, provider or corporate network.

3.2.19 user attribute: A characteristic that describes the user (e.g., user identifier's lifetime, user status as being "available", "don't disturb", etc.).

3.2.20 user identifier: A type of password, image or pseudonym associated with a user, assigned by and exchanged between operators and service providers to identify a user, to authenticate her/his identifier and/or authorize the use of service. Examples are identifiers such as SIP URI, etc.

4 Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

AMR Adaptive Multi-Rate
ANI Application Network Interface
API Application Programming Interface
ATM Asynchronous Transfer Mode
B2B Business-to-Business
CC Content of Communication
CD Compact Disk
cPVR client Personal Video Recorder
DECT NG Digital Enhanced Cordless Telecommunications New Generation
DNS Domain Name System
DTMF Dual Tone Multi-Frequency
EAN Emergency Alert Notification
ENUM tElephone NUmber Mapping
ETS Emergency Telecommunications Service
EVRC Enhanced Variable Rate Codec
HES Hosted Enterprise Services
HTML HyperText Markup Language
IdM Identity Management
IEPS International Emergency Preference Scheme
IM Instant Messaging
IMS Internet Protocol Multimedia Subsystem
IN Intelligent Network
IP Internet Protocol
IPv4 Internet Protocol version 4
IPv6 Internet Protocol version 6
IPTV Internet Protocol Television
IRI Intercept Related Information
ISDN Integrated Services Digital Network
LDAP Lightweight Directory Access Protocol
LEA Law Enforcement Agencies
MMS Multimedia Messaging Service
MPLS Multi-Protocol Label Switching
NAI Network Access Identifier
NAPT Network Address Port Translation
NAT Network Address Translation

NB	Narrow-Band
NGCN	Next Generation Corporate Network
NGN	Next Generation Network
NNA	Numbering, Naming and Addressing
NNI	Network-to-Network Interface
nPVR	network Personal Video Recorder
OAM	Operations, Administration and Maintenance
OIP	Originating Identity Presentation
OMA	Open Mobile Alliance
OS	Operating System
OSA	Open Service Access
OTN	Optical Transport Network
PBX	Private Branch eXchange
PC	Personal Computer
PDA	Personal Digital Assistant
PII	Personally Identifiable Information
PNP	Private Numbering Plan
POTS	Plain Old Telephone Service
PSAP	Public Safety Answering Point
PSTN	Public Switched Telephone Network
QoE	Quality of Experience
QoS	Quality of Service
QoSM	Quality of Service Measurement
RACF	Resource and Admission Control Functions
SIP	Session Initiation Protocol
SLA	Service Level Agreement
SMS	Short Message Service
SR	Service Resiliency
TDR	Telecommunication for Disaster Relief
TE	Terminal Equipment
TIP	Termination Identity Presentation
UC	Unsolicited Communication
UDDI	Universal Discovery, Description and Integration
UMTS	Universal Mobile Telecommunications System
UNI	User-to-Network Interface
URI	Uniform Resource Identifier
USN	Ubiquitous Sensor Network

VoD Video on Demand

VoIP Voice over Internet Protocol

VPN Virtual Private Network

WB WideBand

WiFi Wireless Fidelity

xDSL various types of Digital Subscriber Lines

5 Conventions

In this Recommendation:

The keywords "is required to" indicate a requirement which must be strictly followed and from which no deviation is permitted if conformance to this Recommendation is to be claimed.

The keywords "is prohibited from" indicate a requirement which must be strictly followed and from which no deviation is permitted if conformance to this Recommendation is to be claimed.

The keywords "is recommended" indicate a requirement which is recommended but which is not absolutely required. Thus this requirement need not be present to claim conformance.

The keywords "is not recommended" indicate a requirement which is not recommended but which is not specifically prohibited. Thus, conformance with this specification can still be claimed even if this requirement is present.

The keywords "can optionally" indicate an optional requirement which is permissible, without implying any sense of being recommended. This term is not intended to imply that the vendor's implementation must provide the option and the feature can be optionally enabled by the network operator/service provider. Rather, it means the vendor may optionally provide the feature and still claim conformance with the specification.

For the purpose of this Recommendation, the terms "enterprise network" and "corporate network" can be used interchangeably.

6 Transport

6.1 Transport connectivity

NGN transport stratum [ITU-T Y.2012] is required to use the IP protocol for general, ubiquitous and global public connectivity. The IP protocol may be carried over various underlying transport technologies in the access and core portions of the transport stratum (e.g., xDSL, ATM, MPLS, frame relay, OTN) according to the operator's environment.

NOTE – This does not prevent operators providing technology-specific services directly to users (e.g., ATM, MPLS, frame relay, OTN).

Connectivity is required to accommodate:

1) use of IPv4 and IPv6;
2) real-time and non-real-time communications;
3) one-to-one connectivity;
4) one-to-many connectivity.

6.2 Communication modes

NGN is required to support the following communication modes:

– one-to-one;

– one-to-many;
– many-to-many;
– many-to-one.

6.3 Transport network components

It is an NGN objective to support services and applications independently of the technologies concerning access network and core network. Thus:

1) NGN is required to support diverse access and core transport function technologies.
2) The transport stratum is required to be capable of providing IP connectivity between the end-user functions and core transport functions.
3) NGN is required not to preclude user networks of any level of configuration complexity.

6.4 Network attachments

The following requirements related to network attachment apply:

1) NGN is required to support registration at the access network level, initialization of end-user functions for accessing the NGN services and management of the access network IP address space, including a NAT function.
2) The user profile is required to keep user access authentication data and information related to the required network access configuration.
3) NGN is required to support the re-configuration of services available to the user when the user is nomadic and accesses their services from a location other than the subscribed-to location. Services may be dependent on any or all of: the user device, the access network and arrangements (e.g., roaming agreements) between the service provider and the access network provider. The access network is required to allocate resources according to the services to be provided.
4) When multiple access networks are connected to a single NGN core network, an access network is required to be able to authenticate/authorize access by a user roaming on this access network from another access network.
5) To guarantee the availability of roaming services, the NGN access network attachment procedures are required to support access network authentication based on a standardized method for identifying users at access network level (e.g., the network access identifier (NAI) mechanism specified in [b-IETF RFC 2486]).

6.5 IPv6 support

IPv6 supports not only extensions of IP address space but also various advanced features which influence NGN functions and relevant functional entities. That is, IPv6 also has more flexibility for introducing new applications/services using the combination of extension headers and options.

Therefore, this clause identifies general requirements of IPv6-based NGN which are influenced by IPv6 features. It is recognized that IPv6-based NGN is required to satisfy the following requirements:

– IPv6-based NGN is required to support the IPv6 extension headers and options;
– IPv6-based NGN is required to accommodate IPv6 addressing schemes.

6.5.1 Multi-homing for IPv6-based NGN

– IPv6-based NGN is required to support multiple access capabilities for a user, including access capabilities to access networks using different technologies (e.g., mobile network, WiFi).

– A user terminal is required to have multiple connections with multiple network interfaces and/or multiple IPv6 addresses.
– A user terminal using multi-homing with IPv6 is recommended to acquire (or relinquish) additional IPv6 addresses dynamically.
– A user terminal using multi-homing with IPv6 is recommended to acquire (or relinquish) additional network interface(s) dynamically.
– IPv6-based NGN is required to acquire (or relinquish) additional IPv6 prefixes dynamically.

6.5.2 Signalling in IPv6-based NGN

1) IPv6-based NGN is required to support signalling interworking with other networks (e.g., IPv4-based NGN).
2) IPv6-based NGN is required to support signalling minimizing required modifications for signalling protocols used in IPv4-based NGN.

6.5.3 IPv6 migration in NGN

NGN is required to support IPv6 migration function in access transport functions or core transport functions.

6.6 Multicast support

These capabilities enable applications to deliver content to multiple users at the same time.

In addition to unicast, multicast capabilities are required to be supported for efficient network resource usage and scalable data delivery.

The following requirements apply to NGN:

1) It is required to provide multicast-based capabilities in a single NGN domain.
2) It is recommended to provide multicast-based capabilities across multiple NGN domains.
3) NGN is required to provide multicast data delivery capabilities.
4) NGN is required to provide multicast service control capabilities.
5) NGN is required to support multicast group management capabilities.
6) NGN is required to support security mechanisms for multicast.
7) NGN is required to support nomadism for multicast communications.
8) NGN is recommended to support pre-defined, multicast group-wide QoS capabilities without QoS negotiation support.
9) NGN is recommended to support seamless mobility for multicast communications.
10) NGN can optionally support reliability for multicast capabilities.

NOTE – For further details, see [ITU-T Y.2236].

7 Service and application support

7.1 Open service environment

7.1.1 General requirements for open service environment

Open service environment capabilities stem from the general characteristics of the NGN in supporting and establishing an environment for enhanced, flexible and open service creation and provisioning within the service stratum.

Implementing new functionalities in current networks may be limited or impossible due to the capabilities of the installed equipment. Software provisioning to implement new functionalities is essentially restricted to equipment vendors, since the application programming interfaces (APIs) are typically proprietary (i.e., not open).

NGN is required to enable new capabilities and support a wide range of emerging services, including services with advanced and complex functionalities. Due to a drive from third-party application and service providers to develop new applications and capabilities accessible via open and standard interfaces, there is an increasing need for network and service providers to cooperate in the development of standard application network interfaces (ANIs). Furthermore, software reusability and portability, and use of commercial software, are recommended to be supported to facilitate cost effective development.

Some general benefits of an open service environment are as follows.

– Applications and capabilities can be easily developed by network providers as well as by third parties.
– Capabilities can be made portable and/or reusable across networks.
– Open and standard ANIs will accommodate interactions between NGN entities and applications (e.g., for service creation).

Within an open service environment, each capability is required to be able to function either independently or in conjunction with other capabilities for the realization of applications. Each capability performs all corresponding service functions for the requesting entity (e.g., third party). Applications may be provisioned in different networks, so the capabilities have to be able to function independently from the underlying network technologies.

NGN is required to satisfy the following open service environment general requirements:

1) Independence from transport network providers: Functionalities, operations and management of applications and services are required to be independent from the underlying transport network providers' infrastructure and network technologies.
2) Independence from manufacturers: A multi-vendor open service environment is required to be supported, providing users with a wide range of services and applications in a competitive environment.
3) Location transparency: In a distributed environment, service providers are required to be able to access capabilities from anywhere, regardless of the actual physical location of such capabilities.
4) Network transparency: The open service environment is required to allow applications and services to be technology- and terminal-agnostic.
5) Protocol transparency: Protocol transparency is required to be achieved by providing open standardized protocol programming interface tools for realizing independent service control process and shielding complex network technical details to the open service environment.
6) Secure access to open service environment capabilities is required to satisfy the general NGN security requirements as specified in clause 10.

NOTE – Additional requirements to support an open service environment are provided in [ITU-T Y.2234]

7.2 Service enablers

The "service enablers" category groups capabilities providing features for specific or advanced services and applications, and/or enabling access to, and/or handling of, the specific information provided by these same capabilities.

NOTE – Appendix II provides an example mapping of selected services to selected service enablers.

7.2.1 Group management

This capability provides functionalities related to the secure and efficient management of groups of network entities (terminals, users, network nodes, etc.). It may be used by applications and services for different purposes, including VPN applications, video content distribution, device management, transport and service provisioning and management, emergency (community notification) services, etc.

A typical case which requires group management is a VPN service provided by a provider. In the VPN case, a closed group has to be defined with a member list of service users, and communications within this group is recommended to be securely protected from other users. NGN is recommended to manage such groups and provide secure group communications.

Another example is simultaneous distribution of video content by multicast from a source to multiple users in a group. For such an application, the group management capability is also essential. Requirements of group management are as follows:

1) NGN is required to provide a capability which enables the creation of transport stratum groups.
2) NGN is required to provide a capability which enables the creation of service group and/or service-specific groups (service stratum).
3) NGN is required to manage groups, and provide secure group communications.

7.2.2 Personal information management

This capability provides management of application-specific static and dynamic information (user-related and communication-context-related). Examples of application-specific information include user contact information, application membership (passwords, etc.), default application parameters, bandwidth/QoS preferences (e.g., according to available access networks), media preferences, user-specified data, etc. Delivered by applications (e.g., notification and information services) according to pre-defined user preferences and policy attributes (e.g., across various mobile devices and access network types), this information may be stored and managed by the personal information management capability on behalf of the users. The personal information management capability, acting as user proxy with respect to applications, may also retrieve this information from applications on behalf of the users.

The following are requirements for the personal information management capability:

1) A personal information management capability can optionally be provided. The personal information management capability may store and manage application-specific static and dynamic information on behalf of the users; it may also retrieve this information from applications on behalf of the users.
2) The information managed by the personal information management capability is required to be protected against unauthorized access/retrieval or manipulation, etc.
3) The personal information management capability is recommended to support different communication contexts.

7.2.3 Message handling

In today's networks, some services are supported in both wired and wireless environments, others are only found in one. For example, short message service (SMS) has been designed for a wireless environment, although it can now be found in some fixed networks, whereas instant messaging (IM) has been designed for a wired environment, although some mobile networks have implemented IM services. The expectations of the various services also differ in that some services are designed to be used in what is perceived as 'real time' and others are designed as a 'mailbox' service where the message is stored ready for delivery at a later time.

The message handling capability provides functionalities for message-based services. Functionalities include real-time and non-real-time messaging service control. Examples of real-time messaging are IM and Chat, non-real-time examples being electronic mail, SMS and multimedia messaging service (MMS).

General requirements are as follows:

1) NGN message handling capability is required to support messaging services accessible by both types of terminals, those which are for use of wired transport access and those for use of wireless transport access.

2) NGN message handling capability is required to support both real-time and non-real-time messaging services.

NOTE – The group management capability may be also necessary for supporting messaging services.

In addition, there are user requirements for the message handling capability to enable configuration features of messaging services, such as selection, filtering, formatting, group management and processing (e.g., isolation of unsolicited bulk telecommunications).

7.2.4 Presence

The presence capability (service) provides access to presence information and its availability to users or services. Presence is a set of attributes characterizing the current properties (e.g., status, location, etc.) of an entity.

An entity in this respect is any device, service, application, etc., that is capable of providing presence information. Availability, on the other hand, denotes the ability and willingness of an entity to communicate based on various properties and policies associated with that entity – e.g., time of day, device capabilities, media preferences and capabilities, etc. The terms "presence" and "availability" are almost always used together to provide a complete set of presence information.

NGN is required to support both a user as the supplier of presence information (sometimes called presentity [b-ETSI TR 121 905]), and a user as the requester of presence information (watcher).

Presence is enabled by three capability groupings. Requirements for each capability grouping are described below.

Presence collection

1) NGN is required to provide a capability to collect information describing the connectivity state of the presentity on permission of the user, e.g., the device(s) used by a user.

2) NGN is required to provide a capability to collect information concerning the location of the presentity according to national regulations and laws.

3) NGN is required to provide a capability to collect the information concerning multimedia content of the presentity.

4) NGN is required to provide a capability to aggregate the presence information of multiple presentities.

Presence distribution

5) NGN is required to provide a capability to enable an entity, e.g., a user, to be informed of current presence status of the presentity. Another example is the usage of this capability to enable another service to access the users' presence information depending on the permission of the user.

6) NGN is required to provide a capability to distribute the information concerning multimedia content of the presentity.

7) NGN is required to provide a capability to send the notifications in bulk for multiple presentities.

8) NGN is required to distribute the presence information based on expiration time (duration), which can be one time event or validity period.

Presence management

9) NGN is required to provide presence management, a set of capabilities to manage the presence information collected.

10) Access control to the presence information (using the presence distribution capabilities) is required to be managed in compliance with presentity privacy and access rules requirements.

11) The presence management capabilities are required to enable the distribution capability to supply only part of the presence information where required.

12) The presence management capabilities are required to enable collection of requests from certain entities to receive presence information for other entities. The presence management also provides the presentity with the ability to determine the distribution of its presence information, e.g., to accept or reject requests for presence information on a per watcher basis.

7.2.5 Location management

Location management is an enabling capability for provisioning of location-based applications and services, which use information regarding the location of users and devices within networks. The location of users and devices within networks may be related to their physical positioning, hence enhancing applications with local context and relevance.

Mechanisms to determine and report location information often depend on the access network technology. This means that support for location-based applications and services are recommended to be implemented within each access network technology.

The following are requirements for location management:

1) NGN is required to provide a location management capability to determine and report information regarding the location of users and devices within NGN according to national regulations and laws.

2) NGN is required to provide additional functionalities to ensure the correctness and authenticity of location information used by applications and services to mitigate any adverse effects due to fraudulent or false location information.

3) Privacy issues are required to be fulfilled by provisioning location-based services and applications.

4) The location management capability is required to provide a means to release location information according to the information contained in user/device profiles.

7.2.6 Push

Push is an enabler that provides the capability to transmit data from a sender to a recipient without previous request by the recipient, e.g., via SIP-based push mechanisms.

Whereas the user typically has the ability to configure push services from a range of services provided by service providers, the recipient does not have to issue a specific request but a general request for the data to be sent. Data can be sent either as a result of a single invocation application-dependent trigger or periodically.

As an example, push may be used to provide notification that an MMS message is available.

The push requirement is as follows:

1) NGN is required to support a push capability according to national regulations and laws.

NOTE – Invocation of push services may require user agreement.

7.2.7 Device management

Device management is an enabler that provides the network capabilities to manage and control devices. Device management capabilities may be used for:

– hardware/software configuration management, such as device hardware information, media capabilities, software version;

– remote software upgrades, both with and without user intervention, such as bug-fixes, features, OS, firmware, application clients;

– remote fault diagnosis.

General requirements for device management are as follows:

1) NGN is required to support device upgrades.

2) NGN is required to support device auto-configuration.

3) NGN is required to support gathering device connection information according to national regulations and laws, such as IP address and location.

4) Device management can optionally provide functions for registering, managing and updating device information.

5) Device management can optionally provide functions for remotely checking device status, including status changes and upgrades, and generating diagnostic reports.

6) Device management procedure is required to be secure, always carried out by a trusted entity according to national regulations and laws.

NOTE 1 – Device management is recommended to allow installation of user preferences and applications.

NOTE 2 – Invocation of device management services normally requires user agreement.

7.2.8 Session handling

NGN is required to provide the capabilities to set up, manage and terminate end-to-end service sessions that involve, for example, multiple parties, a group of endpoints associated with those parties, and a description of multimedia connections among the endpoints. These session-handling capabilities are required to be provided in both fixed and mobile environments in order to accommodate different service requirements, as well as to use the appropriate application servers for service operation.

The session handling functions include:

– session establishment;

– presentation of the identifier of originating party and connected-to party of a session;

– suppression of the identifier of originating party and connected-to party of a session;

– delivery and suppression of user-provided optional information (e.g., picture, video or text during session establishment);

– handling of an incoming session by the terminating party;

– negotiation of capabilities for an incoming session;

– accepting, ignoring, re-directing or rejecting an incoming session;

– negotiation of media and media components during session establishment;

– handling of an ongoing session;

– modification of media and media components in an ongoing session;

– suspending and resuming an ongoing session;

– ending a session;

– network-controlled session termination.

General requirements for session handling are as follows:

1) Session handling is required to be able to use the appropriate application servers for service operation.
2) NGN is required to support the users' ability to invoke one or multiple sessions, and to activate concurrent multimedia applications within each session.
3) Session handling is required to support sessions with a variety of media types (voice, video, text).
4) Session admission control based on defined levels of QoS and security is required to be supported.
5) Session admission control mechanisms are required to span multiple services (e.g., voice, text, video).
6) If there are one or two participants in the session, the network is required to end a session at any time during the session, when requested by any of the session users. The network can optionally end a session at any time during the session (e.g., in failure conditions).
7) If there are more than two participants in the session, the network can optionally end a session at any time during the session, when requested by any of the session users. The network can optionally end a session at any time during the session (e.g., in failure conditions).

7.2.9 Web-based application support

The web-based application support enablers allow enhanced utilization of device capabilities and network characteristics for web-based applications.

Web-based application support capabilities provide users with a consistent web environment which spans multiple network environments and multiple devices (PC, laptop, PDA, cell phone, etc.).

Web-based application support includes the following interactions:

– (application) server-to-server;
– server-to-terminal;
– terminal-to-server;
– terminal-to-terminal (or peer-to-peer).

NGN is required to provide web-based application support satisfying the following:

1) interoperability across wired and wireless network environments;
2) secure access to applications;
3) nomadism;
4) low time delays and efficient bandwidth use.

NGN is recommended to provide web-based application support satisfying the following:

5) re-use of existing technologies and NGN components (e.g., authentication) for web-based application provisioning;
6) re-use of authoring and integration tools;
7) consistent user experience across networks;
8) support of service composition techniques;
9) scalability of web-based applications;
10) non-degradation of NGN reliability.

NOTE – NGN may be limited in respect of web-based application support capabilities.

7.2.10 Data synchronization

Data synchronization is defined as the act of establishing equivalence between two data sets. The data synchronization enabler synchronizes networked data of different terminals, including handheld computers, mobile phones, laptop PCs and desktop PCs. Applications which may utilize the data synchronization enabler include calendar, contact information management, management of enterprise data stored in databases, and management of web documents.

NGN is recommended to support a data synchronization enabler with the following features:

1) synchronization of networked data with terminals supporting this capability;

2) synchronization of a terminal with appropriate networked data;

3) synchronization of networked data among terminals.

If a data synchronization enabler is supported, the following requirements apply:

1) The data synchronization enabler is required to be independent from transport protocols.

2) Arbitrary networked data is required to be supported.

3) Data synchronization is recommended to be aware of the resource limitations of terminals.

7.3 Context awareness

Context awareness is a capability to determine or influence a next action in telecommunication or a process by referring to the status of relevant entities, which form a coherent environment as a context. The status of individual entities and their status aggregation are treated as context information. Examples of context information are subscriber's connectivity, the location of remarked goods in a distribution system and traffic status in a network.

The following key roles are assumed:

- **Context generator**: It generates context information and permits access to it. Context generator can be inside NGN or outside NGN.
- **Context requestor**: It requests context information and refers to it. It can be inside NGN or outside NGN.
- **Context distributor**: It collects, distributes, processes and optionally stores context information, acting as a mediator between context generator and context requestor.

When the roles above are performed by NGN, NGN is recommended to provide:

1) Security for context information from the context generator point of view:
   - It is required that the context information be accessed by context requestor(s) only when the context generator allows it to do so. This policy is required to be maintained as long as the context information is alive in NGN.
   - Unintentional tracking for a context generator is required to be prohibited.

     NOTE – This requirement assumes a case where context information from a context generator is open to different context requestors for different purposes. It has to be related only to intentional usage. For example, although a context generator permits a user to access his/her book purchase history (in order to get information on possible new releases), this information is required to be prohibited from being accessed by other applications such as advertisement distribution for movie tickets, music CDs or sportswear.
   - Context information in a distribution process in NGN is required not to be leaked or abused.
   - Context information stored in a database in NGN is required not to be leaked or abused.

2) Reliability of context information from the context requestor point of view:
   - Context information is recommended to be transparently transferred to the context requestor without being changed.
   - The newest context information is recommended to be transferred to the context requestor.
   - It is desirable that old context information is automatically abandoned.
   - Fake context information is required to neither be generated nor be opened.
3) Simple usage of context information to be kept from the context requestor/application provider point of view:
   - Data format and semantics of context information is recommended to be standardized in order that various context requestors/application providers can use them.
   - Context information is recommended to be easily searched by context requestor, if permitted.
   - Context information is recommended to be used by context requestor at any time, if permitted.
   - The primary context information can optionally be converted into appropriate context information in order that an application provider can easily develop an application by using the converted context information.
   - Context distributor can optionally be able to automatically select service elements and data among a lot of alternatives in order that a third party application developer can easily develop an application by using context information.
4) Context information to be transferred in real time and on demand manner if the context requestor desires.
5) Scalability of context distributor:
   - Huge amount of context information is recommended to be handled in order to avoid false inference based on limited context information.
   - Context distributor is recommended to be flexible to handle various types of context information and to support various applications.
6) Efficient distribution of context information.

8 Routing

NGN is required to provide capabilities to select the proper routing paths between the traffic originating endpoint and the traffic receiving endpoint.

NGN is required to support the routing schemes most suitable for NGN providers. In particular, NGN is required to support:

1) both static and dynamic routing schemes;
2) routing schemes which can effectively operate within an NGN domain;
3) routing schemes which can effectively operate between NGN domains, thereby allowing interoperability;
4) routing based on ITU-T E.164 number ranges.

NGN is recommended to support:

5) context aware based routing (for example, routing based on the presence, location and personal information).

NOTE – Clause 7.3 provides further information about context awareness.

9 Quality of service

NGN is required to support end-to-end QoS across different networks of varying infrastructure technologies provided by multiple operators to ensure the required service level for users or applications. NGN is required to support multiple levels of QoS, which may be negotiable between the user and provider and/or between providers. QoS service level support includes use of resource and admission control mechanisms, traffic class differentiation, priority management, QoS signalling mechanisms, performance measurement and management for quality insurance, and overload/congestion control.

9.1 General QoS requirements

NGN is required to meet the following QoS requirements:

1) Allow different technologies and business models.
2) Support the different processes related to service lifecycle (e.g., subscription/provisioning, invocation, monitoring).
3) Support different terminal equipment capabilities (for example, some terminal equipment may support transport stratum QoS signalling, while others may not).
4) Control the QoS-related transport resources within packet networks and at the network boundaries in accordance with their capabilities [ITU-T Y.2111].
5) Support resource and admission control within a single NGN domain and between NGN domains.
6) Support both relative QoS control and absolute QoS control [ITU-T Y.2111].
7) Support application-driven QoS requirements.
8) Verify transport resource availability on an end-to-end basis [ITU-T Y.2111].
9) Support QoS differentiation over various categories of packet traffic including packet-type flows and user designations [ITU-T Y.2111].
10) Authorize requests for QoS and operate only on the authorized requests for QoS [ITU-T Y.2111].
11) Support dynamic near-end NAPT control and firewall working mode selection [ITU-T Y.2111].
12) Support far-end (remote) NAT traversal [ITU-T Y.2111].
13) Provide resource and admission control for multicast in support of, e.g., IPTV [ITU-T Y.2111].
14) Provide resource and admission control in support of nomadicity [ITU-T Y.2111].

9.2 Network QoS classes

1) NGN is recommended to take into consideration the network performance at the transport stratum.
2) NGN is recommended to support NGN QoS classes based on [ITU-T Y.1541].

9.3 Service/application priority

NGN is recommended to support service/application priority as follows:

1) priority classification schemes for admission control and restoration;
2) signalling extensions that indicate priority levels across UNI, NNI and ANI;
3) priority enabling mechanisms that deliver the desired priority action.

9.4 QoS control

NGN is recommended to support:

1) per-flow, per-session, per-service-class QoS control granularity;
2) dynamic QoS behaviour (i.e., it is recommended to be possible to modify QoS attributes during an active session);
3) QoS resource control based on a distributed, centralized or a hybrid approach;
4) admission control and congestion control mechanisms;
5) mechanisms to guarantee the timely and reliable delivery of signalling and control packets;
6) mechanisms to prioritize the delivery of emergency telecommunications and priority telecommunications;
7) methods for resource-based admission control, e.g., using performance measurement information.

9.5 QoS signalling

NGN is recommended to use signalling mechanisms to support QoS.

Detailed requirements for QoS signalling are out of scope of this Recommendation and contained in other specific Recommendations.

9.6 Performance

NGN is required to provide performance measurement and management to ensure QoS.

The network performance measurements and their management are recommended to support:

1) providers' assurance of performance delivery (for comparison against SLAs);
2) providers to supply performance information for prospective customers;
3) providers' troubleshooting among their networks along defined paths;
4) providers' internal indication of performance impacts due to changes within their networks;
5) providers' monitoring of each other's network performance;
6) providing information to other NGN functions, e.g., RACF.

Detailed requirements for performance measurement and management are out of scope of this Recommendation and contained in other specific Recommendations.

9.7 Processing and traffic management

In order to avoid processing and traffic overload and to keep response times reasonably low under such overload to preclude users abandoning their service requests, NGN is recommended to provide mechanisms for overload detection and control (including expansive controls such as load balancing and resource replication) within both the service and transport strata.

NGN is recommended to have mechanisms available to control overload that:

1) convey indication of overload conditions and the degree of overload to other networks;
2) optimize effective throughput (e.g., admitted service requests/s or packets/s) subject to service priority considerations at an overloaded resource;
3) achieve this throughout the duration of an overload event, irrespective of the overloaded resource's capacity or of the number of sources of overload;
4) allow the network that receives the overload indication to control its traffic.

10 Identification and security

NOTE – The use of the term 'Identity' in this clause does not indicate its absolute meaning. In particular, it does not constitute any positive validation of a person.

10.1 General requirements for identification, authentication and authorization

The requirements in this clause are not tied to any specific set of NGN services or applications.

NOTE 1 – Specific authentication and authorization mechanisms are out of scope of this Recommendation.

There are requirements for bilateral identification, authentication and authorization capabilities in both the transport and the service stratum. In the transport stratum, there are requirements on how NGN transport resources can be used. In the service stratum, requirements are on the association between a user and a service or between a user and another user, including the case when the two users are on different NGNs.

NOTE 2 – Sometimes the phrase "service provider" has been used to refer to the provider of transport stratum services. In this clause, the network provider is usually shortened to "(the) NGN", and the "service provider" is exactly that, the "provider of the service": the service provider could be anywhere, and is not necessarily the network provider.

The following are general requirements for identification, authentication and authorization capabilities.

1) NGN is required to support bilateral authentication and authorization functions for both the transport and the service strata. Transport stratum authentication requires a user to be identified by the network in order to obtain access to the network and to privileged uses. An authentication function can be a significant factor in protection from unauthorized use of networks, such as prevention of unsolicited bulk telecommunications. An authorization function can set up access to network resources and prevent access violations.
2) NGN is required to uniquely identify users by one or both of the following types of user identifier:
   – Public user identifier: The information that is normally used by one NGN user to contact or communicate with another NGN user.
   – Private user identifier: A private NGN user identifier can be used to identify the NGN user to her/his NGN network or service provider. The private user identifier is one component used for authentication.
3) NGN is required to allow separate identification, authentication and authorization of users and terminal equipment.
4) NGN is required to allow verification of the association between the user and the user's terminal equipment for some specific services.
5) Authentication, authorization and accounting, performed by the NGN provider and the service provider, is recommended to be processed securely.
6) A service provider is required to provide mechanisms that allow presentation of the public identifier of the communication originator, where appropriate and where permitted.
7) A service provider is required to provide mechanisms to withhold the public identifier of the communication originator, if the presentation of this information is restricted by the communication originator or the network.
8) A service provider that performs authentication is required to support mechanisms to determine the authenticity of a public user identifier presented for an incoming communication.
9) A service provider that performs authentication is required to provide mechanisms that allow the presentation of the public user identifier of the connected party to the

communication originator, if applicable, and if this is not restricted by the connected party or the network.

10) NGN is required to be able to verify the private identifier of users and terminals (if applicable). Additionally, it is required to be able to check the authentication and authorization of users and terminals to use resources of the NGN.

11) A service provider is required to be able to verify the private identifier of users of the services it provides. Additionally, the service provider is required to support the capability to check the authentication and authorization of users to use resources it manages.

12) Private and public identifiers of NGN users of transport stratum resources (identifiers used for authentication and authorization) are required to be administered by the relevant network provider.

13) Private and public identifiers of service users of service stratum resources (identifiers used for authentication, authorization and routing), are required to be administered by the relevant service provider and such administration is required to prevent the user from unauthorized changes to the public and private identifiers.

14) Private NGN user identifiers provided for authentication and authorization are required to be withheld from other users.

15) Public NGN user identifiers of service users can optionally be visible to other users if no service intermediaries are involved and the user's permission is given.

16) A service provider can optionally allow a user to access a service from multiple terminals in parallel using the same public and private user identifier.

17) As a single user may use multiple private user identifiers via a single subscription procedure, the NGN is required to support multiple private user identifiers via a single subscription procedure.

18) NGN can optionally authenticate and authorize a single user for multiple services ("single sign-on").

NOTE 3 – Even when only a single authentication event is required, multiple authorization events may still be needed. In addition, single sign-on can be implemented on the client side, such that even though multiple authentications are required, the human user only needs to establish an authentication relationship once. NGN does not require support of single sign-on capabilities. However, where such support exists with current technologies, it is expected to be also used for NGN.

Authentication of a subscriber's identifier or of a user's identifier is not intended to indicate positive validation of a person.

10.2 Requirements for identification

NGN provides capabilities for user identification, in order for network operators and service providers to identify the users of certain NGN services and use this information as required (e.g., for authentication and authorization procedures). NGN is required to provide capabilities for the user to identify NGN providers (on each stratum) where a direct relationship exists.

Requirements for identification capability include the following:

1) Multiple user identifiers

As an NGN user may have one or more public and private identifiers, NGN is required to segregate one identifier from another (e.g., for personal use and business use).

2) Identifier portability

NGN is required to provide capabilities that provide the equivalent of number portability in PSTN environments.

3) Identifier independency

The public user identifier is recommended to be assigned to the user independent of its repository, the user terminal and the underlying network technologies. However, backward compatibility (e.g., for a POTS handset) can optionally be achieved via proper interworking functions.

4) Support for identifier attributes

Private identifier attribute, such as the lifetime of that identifier for the user, the subscriber, the network in use, etc., can optionally be associated with a user identifier.

5) Support for attribute conditions

Conditions (e.g., setting timer as validity conditions) for a user attribute can optionally be associated with a user identifier by an attribute provider (e.g., network, principal user, end user).

6) Selective attribute authorization

NGN is required to support selective authorization of user's private identity attribute information by an attribute provider (e.g., identifier lifetime).

7) Support for subscriber programming

NGN is recommended to support subscriber's programming of different permissions for different attribute information, e.g., access to and usage of private identity attribute information, on a per attribute basis.

8) User and terminal binding

NGN is required to support a dynamic binding of the public user identifier and the terminal equipment identifier for certain services.

9) Multiple terminal associations

NGN is required to allow association of a user public or private identifier to multiple (mobile or fixed) terminal equipment identifiers for certain services. The user may be allowed to use multiple terminals at any given time.

10) Identifier information transfer

NGN is required to support the transfer of the user identifier information by NGN users if permission is given by the user providing input either on their own terminal or on the receiving terminal for certain services (e.g., point of sale terminal).

11) Public user identifier administration

A public user identifier is required to be administered by the network operator and is required not to be changeable by the user.

12) Public user identifier authenticity

The network operator is required to guarantee the authenticity of a public user identifier presented for an incoming session to a user where the communication is wholly across a trusted network.

10.3 Requirements for authentication

Authentication is the process of establishing confidence in user and terminal equipment identifiers as well as network attachment and service offers. From the point of view of providers, NGN may distinguish between transport network authentication and service authentication. From the perspective of subscribers, NGN may distinguish between user authentication and terminal equipment authentication. Network authentication is the process of verifying user/terminal equipment identifiers for transport network access only by network providers. Service authentication is responsible for verifying user/terminal equipment identities for service usage

purpose. From the perspective of subscribers, NGN is required to provide the capability for a user to authenticate and identify a transport network provider.

From the perspective of subscribers, NGN is also required to provide the capability for a user to authenticate and identify a service provider.

NGN is recommended to allow for these capabilities to be independent.

These distinct authentication concepts may be unified into a single concept or be applied separately, depending on the transport technology or business model. For example, a single authentication flow may be processed if a network provider is also a service provider.

Requirements for authentication capability include the following:

1) NGN is required to allow various network authentication mechanisms appropriate to the underlying access network technologies.
2) Service authentication is recommended to aim to be independent of the NGN access network technologies and maintain a consistent service authentication mechanism.
3) NGN is required to request user/terminal equipment to input authentication information either in an explicit or implicit manner.
4) NGN is recommended to support both software-based and hardware-based authentication mechanisms.
5) Terminal equipment authentication that uses device profile information is required to be supported.
6) NGN is recommended to provide capabilities of bilateral authentication between service provider and user.
7) NGN is recommended to provide capabilities of bilateral authentication between transport network provider and user.

10.4 Requirements for authorization

Requirements for authorization capability include the following:

1) NGN is required to provide service access to authenticated users and/or devices based on their access rights, user profiles and network policy.
2) Service authorization is recommended to aim to be independent of the NGN access network technologies.
3) Authorization capability is recommended to support NGN mobility scenarios where applicable.

10.5 Identity management

1) NGN is required to support a structured approach for identity management (IdM) of the identity (identities) (including associated information such as identifiers, attributes, assertions and policy) for entities such as:
   a) Users/groups.
   b) Organizations/federations/enterprises/service providers.
   c) Devices/network elements/systems.
   d) Objects (application process, content, data).
2) NGN is required to support IdM capabilities to allow:
   a) Secure management of the lifecycle (e.g., registration, validation, revocation) of an entity's identity (identities).

b) Secure discovery and exchange of identity information associated with an entity's identity (identities). This includes discovery and exchange of identity information that is located within an NGN domain and across different NGN domains.

3) NGN is required to support capabilities for enforcement of applicable policy associated with an entity's identity or identity information.

4) NGN is required to support common IdM capabilities to be used by multiple services and applications, including:

   a) Real-time communication services (e.g., VoIP, linear TV and real-time messaging services).

   b) Other communication services (e.g., web-based transactions).

5) NGN is required to support IdM capabilities to allow anonymous assertion of identity information (e.g., identifiers and attributes), subject to applicable policy.

6) NGN is required to support IdM capabilities to allow interworking among network elements within an NGN domain (i.e., intra-network) and among different NGN domains or federations. This requires:

   a) Using standard interfaces for exchanging IdM information.

   b) Using standard mechanisms (e.g., protocols, data structures and schemas) for exchanging IdM data.

7) NGN is required to support IdM capabilities to enable end users with ease-of-use features such as:

   a) Single sign-on/sign-off to multiple services and applications.

   b) Fixed and mobile convergence.

   c) Control and protection of personally identifiable information (PII).

8) NGN is required to support IdM capabilities to enable security of services and applications.

9) NGN is required to support security of IdM capabilities, functions, data and communications.

10.6 Security requirements

NGN is required to contain the security features incorporated in existing networks and allow for secure interconnection with other NGNs or non-NGN networks. The requirements are based on the application of [ITU-T X.805] to NGN and thus address the following dimensions of NGN security: access control, authentication, non-repudiation, data confidentiality, communication security, data integrity, availability and privacy.

NGN is required to provide:

1) protection against unauthorized use of network resources and unauthorized access to information flows and applications;

2) authentication of the communication entities if policy requests;

3) mechanisms for data confidentiality;

4) mechanisms for data integrity;

5) a means for accountability, whereby individuals are held responsible for the effect of any of their actions;

6) availability and accessibility of the network, upon demand by an authorized entity;

7) mechanisms of non-repudiation for preventing one of the entities or parties in a communication from falsely denying having participated in the whole or part of the communication;

8) privacy of the user's data, e.g., preferences, profiles, presence, availability and location information. This is required to be protected by revealing information only when valid authorization is provided;

9) protection to minimize the effect(s) of network attacks, from within or outside.

10.7 Critical infrastructure protection

Service providers are recommended to have capabilities to protect their NGN infrastructure from malicious attacks, such as denial of service, eavesdropping, spoofing, tampering with messages (modification, delay, deletion, insertion, replay, re-routing, misrouting or re-ordering of messages), repudiation or forgery. Protection may include prevention, detection and recovery from attacks, and measures to prevent service outages.

Security requirements are provided in clause 10.6.

11 Management

NGN management capabilities support management areas which cover the planning, installation, operations, administration, maintenance, provisioning of networks and provisioning of services. The high-level goal is to provide survivable and cost-effective networks.

NGN management capabilities also support the monitoring and control of NGN services and transport components via the communication of management information across interfaces between NGN components and management systems, between NGN supportive management systems, and between NGN components and personnel of service and network providers.

NGN management capabilities support the aims of the NGN by:

1) providing the ability to manage, through their complete life cycle, NGN components, both physical and logical. This includes resources in the transport stratum and the service stratum, access transport functions, interconnect components and user networks and terminals;

2) providing the ability to manage NGN service components independently from the underlying NGN transport components and enabling organizations offering NGN services (potentially from different service providers) to build distinctive service offerings to customers;

3) providing the management capabilities which enable organizations offering NGN services to offer users the ability to personalize user services and to create new services from NGN capabilities (potentially from different service providers);

4) providing the management capabilities which enable organizations offering NGN service improvements including user self-service (e.g., provision of service, reporting faults, online billing reports);

5) developing a management architecture and management services which enable service providers to reduce the time-frame for the design, creation and delivery of new services;

6) supporting the security of management information, including customer and user information;

7) supporting the availability of management services any place any time to any authorized organization or individual;

8) supporting eBusiness networks based upon concepts of business roles (customer, service provider, complementor, intermediary, supplier (e.g., equipment vendor)) [ITU-T Y.110], [ITU-T M.3050.0];

9) allowing an enterprise and/or an individual to adopt multiple roles in different networks and also multiple roles within a specific network (e.g., one role as a retail service provider and another role as a wholesale service provider) [ITU-T M.3050.0];

10) supporting B2B processes between organizations providing NGN services and capabilities;

11) allowing the management of hybrid networks comprising NGN and non-NGN resources;

12) integrating an abstracted view on resources (network, computing and application), which hides complexity and multiplicity of technologies and domains.

Detailed requirements for NGN management are beyond the scope of this Recommendation and are provided in management-specific Recommendations, such as [ITU-T M.3060].

NOTE – See also the requirements in clause 16.2 "accounting and charging".

12 Mobility handling

Mobility management involves the ability of mobile objects, such as users, terminals and networks, to be able to roam between different networks (NGN or non-NGN). In NGN, two distinct types of mobility are considered: personal mobility and terminal mobility [ITU-T Q.1706].

For NGN, personal mobility exists where users can use registration mechanisms to associate themselves with a terminal that the network can associate with the user. Where interfaces between users and terminals, and users and networks for user registration exist, it is assumed these interfaces will be used for NGN.

For NGN, terminal mobility exists within and among networks where registration mechanisms are used to associate the terminal to the network. Where support for terminal mobility with service continuity exists, such support is expected to also be used for NGN.

The following provides general requirements for mobility management, focused on support of customer needs.

For the services to which mobility is appropriate, NGN is required to provide:

1) nomadism for personal mobility and terminal mobility;

2) mobility support for existing access technologies, existing QoS capabilities and existing security capabilities;

3) location management support for registration, location update and address translation to enable mobility across providers' network boundaries;

4) support for roaming subscription, identification and authentication management;

5) support for security to prevent unauthorized access and ensure user privacy, taking account of service continuity and handover where applicable;

6) support for location confidentiality to conceal location information from non-trusted entities;

7) support for paging capability for set-up of incoming calls, in order to save power in mobile terminals and reduce signalling in the network;

8) support for IP-based mobility management or, at least, well-harmonized with IP technology for their efficient and integrated operation.

For the services to which mobility is appropriate, NGN is recommended to provide:

– support for service continuity for intra-AN and inter-AN scenarios. Service continuity includes the following cases:

  a) service continuity for terminal mobility;

  b) service continuity for personal mobility.

NOTE 1 – Service continuity implementation levels can be different for each scenario depending on conditions, such as access technology restrictions and service level supported by service/network provider.

NOTE 2 – Service continuity for inter-CN (core network) scenarios is for further study.

In case of voice services, NGN is required to support service continuity for terminal mobility.

NGN is required to provide capabilities to support service continuity taking into account network conditions (e.g., the number of user sessions, mobility events and bandwidth consumption) and users' requirements.

NGN is recommended to allow adaptation in order to support service continuity when users' requirements and network conditions mismatch. Adaptation may include negotiation/renegotiation of network QoS and/or terminal parameters (e.g., codec change/adaptation).

NOTE 3 – See [ITU-T Q.1706] for details of the mobility management requirements for NGN.

13 Profile management

13.1 User profile management

A user profile is a set of stored information related to a user (or a subscriber). In an NGN environment, the management of the user profile attributes is especially important since the user information is required to implement a number of capabilities, including authentication, authorization, mobility, location, charging, etc. User profiles include transport-related information and service-related information. User profiles can be stored in separate databases in the service stratum and in the transport stratum and can optionally have data exchange functions between them.

General requirements for a user profile are as follows:

1) For each user, a user profile is required to exist by a related provider, which can optionally consist of several 'components'.
2) These components can optionally be distributed in the home network and service provider's environment; criteria of privacy and data protection are required to be fulfilled.
3) Within the domain of the home network, the components can optionally be distributed in various entities.
4) Within the home network, a functionality that is able to locate user profile components is required. This functionality allows services/applications to be unaware of the actual location of the components and is required to be under the control of the home network.
5) Services, applications and other NGN entities are required to be able to retrieve the related user profile or selected parts of it (as required) in one transaction; criteria of privacy and data protection are required to be fulfilled.
6) Effective means to retrieve individual user profile components are required with acceptable delay for real-time services.

   NOTE – Although user profile management does not attempt to provide any classification of the data a user profile may contain, categorizations such as general user information, service-specific information, etc., can optionally be applied.

The detailed requirements relating to user profile, its usage and management are expected to be contained in further ITU-T Recommendation(s).

13.2 Device profile management

A device profile is a set of stored information related to a user equipment. In an NGN environment, the management of the device profile attributes is also important since the device information is required in conjunction with "user profile" by a number of capabilities, including authentication, authorization, mobility, location, charging, etc. Device profiles may contain transport-related

information or service-related information. Device profiles can be stored in separate databases in the service stratum and in the transport stratum and can optionally have data exchange functions.

NOTE 1 – This information may contain terminal identification attributes like address, name, static attributes such as supported media and protocols, screen details (size in pixels, colour resolution, response time, etc.), transmission speed, bandwidth and processing power, and dynamically changing attributes such as the user using the terminal, geographical location, running applications on the terminal.

Device profiles may be used for the following purposes:

– to track stolen or misappropriated devices;

– to determine the type and level of service that may be provided to the user (based on device capabilities);

– to determine the required quality of service for a connection between terminals (based on device capabilities).

The requirements for device profiles are as follows:

1) For each user equipment, one device profile can optionally exist, which can optionally consist of several "components".

2) These components can optionally be distributed in the home network and/or service provider's environment.

3) Within the home network, the components can optionally be distributed in various entities.

4) Within the home network, a functionality that is able to locate device profile components is required. This functionality allows services/applications to be unaware of the actual location of the components and is required to be under the control of the home network.

5) By endorsement of the user, services, applications and other NGN entities can optionally be able to retrieve the whole device profile or selected parts of it (as required) in one transaction; criteria of privacy and data protection are required to be fulfilled.

6) An effective means to retrieve individual device profile components is required with acceptable delay for real-time services.

NOTE 2 – Although device profile management does not attempt to provide any classification of the data a device profile may contain, categorizations such as general device information, service-specific information, etc., can optionally be applied.

The detailed requirements relating to device profile, its usage and management are expected to be contained in further ITU-T Recommendation(s).

14 Media handling

14.1 Media resource management

Media resource management mechanisms are traditionally used in conjunction with traditional voice processing services and user interactions via voice and DTMF. These have to be expanded in NGN in support of new data, video and content services.

NGN is required to support various media resources and media resource management capabilities to enable a wide range of applications.

Media resource capabilities for NGN include:

– media recording (e.g., to support voice mail service);

– playing recorded media (e.g., to play voice mail, tones and announcements);

– DTMF recognition (e.g., to support interactive voice response services);

– advanced speech recognition (e.g., to support interactive voice response services);

– media conversion (e.g., to support text-to-speech, speech-to-text and fax-to-email services);
– transcoding;
– video/text/audio/data bridging (e.g., to support conferencing services);
– media duplication (e.g., to support lawful interception);
– media insertion.

Additional media resource capabilities for NGN include:

– media downloading (e.g., video/audio clips, pictures);
– media streaming (e.g., video on demand);
– transparent transferring;
– distributed media storage and delivery (multiple copies of media, multiple segments of media);
– dynamical media addressing (locating the existed media on proper media storage for user's media access in real-time).

14.2 Requirements for codecs

14.2.1 General

General requirements for codecs for NGN include the following:

1) Transcoding is required to be avoided wherever possible.
2) NGN is required to support end-to-end negotiation of any codec between NGN entities (terminals, network elements). It is the responsibility of entities at the rim of an NGN (e.g., NGN terminals and user equipment) and network equipment originating and terminating the IP media flows, to negotiate and select a common codec for each "end-to-end" media session. NGN is required to support end-to-end negotiation of text codecs, such as those currently specified in ITU-T Recommendations.

The following features of codecs for NGN are recommended:

1) self-adaptive operation to varying QoS conditions;
2) dealing with the effects of service level changes on codec operation;
3) compatibility with PSTN/ISDN codecs;
4) discovery/interrogation of codec parameters;
5) selection/negotiation and mid-session renegotiation of codec parameters.

14.2.2 Audio codecs

The following audio codec classes are envisaged:

a) "narrow-band audio" for audio range of 300 Hz to 3400 Hz;
b) "wideband audio" for audio range of 50 Hz to 7000 Hz;
c) "super wideband audio" for audio range of 50 Hz to 14000 Hz;
d) "full band audio" for audio range of 20 Hz ~ 20,000 Hz, with associated multichannel capabilities (mono, stereo, etc.).

In order to enable interworking between the NGN and other networks (including the PSTN, mobile networks and other NGNs) the NGN must be capable of receiving and presenting [ITU-T G.711] coded speech when interconnected with another network. When a packetization size is not selected by codec negotiation between terminals and/or network elements or agreed by bilateral arrangement, a speech packetization size of 10 ms samples is recommended to be used for ITU-T G.711 coded speech; this is recommended as an optimum value balancing end-to-end delay

with network utilization. It is recognized that there can optionally be network constraints which require that a higher value be agreed by bilateral arrangement; in such cases, a value of 20 ms is recommended.

NOTE 1 – Where a packetization size is selected by codec negotiation between terminals and/or network elements, this Recommendation places no requirements on the value to be selected.

NOTE 2 – The above does not make any requirement about the codecs to be supported by terminals nor does it mandate that NGN is required to support audio transcoding between any arbitrary codec to [ITU-T G.711].

In addition, support for the following audio codecs is recommended:

– AMR [ETSI TS 126.071]: In order to support 3GPP terminals and to facilitate interworking with 3GPP networks.

– ITU-T G.729A [ITU-T G.729]: In order to facilitate interworking with existing VoIP networks and support existing VoIP terminals.

– EVRC/EVRC-B [TIA-127-C]: In order to support 3GPP2 terminals and to facilitate interworking with 3GPP2 networks.

14.2.3 Wideband audio codecs

14.2.3.1 General

Clause 14.2.1 is required to take precedence over this clause, to reduce transcoding and improve both wideband interoperability and end-to-end quality.

Wideband audio is an optional capability that can be supported by:

– entities at the rim of the NGN (e.g., NGN-TE) which have a wideband audio ability;

– network equipment originating and terminating the NGN IP media flows with wideband audio content.

Terminals providing wideband audio capabilities are required to also have NB capability and comply with clause 14.2.2.

Network equipment providing wideband audio capabilities are required to also have NB capability and comply with clause 14.2.2.

Audio transcoding can optionally be performed to provide end-to-end service interoperability, but this is recommended to be avoided wherever possible.

14.2.3.2 Wideband audio codecs in terminals

Terminals originating and terminating end-to-end IP media flows in NGN, supporting wideband audio is recommended to provide one or more of the following wideband audio codecs:

– ITU-T G.722 [ITU-T G.722];

NOTE 1 – Required for DECT NG user equipment, used in some VoIP and/or legacy user equipment.

– AMR-WB/ITU-T G.722.2 [ITU-T G.722.2];

NOTE 2 – Required for 3GPP user equipment and/or user equipment with mobility according to 3GPP access.

– ITU-T G.729.1 [ITU-T G.729.1];

NOTE 3 – Used in some DECT NG user equipment, some VoIP and/or legacy user equipment.

– EVRC-WB [TIA-127-C].

NOTE 4 – Required for 3GPP2 user equipment and/or user equipment with mobility according to 3GPP2 access.

NOTE 5 – Terminals can optionally provide any other codecs in addition to the above list.

NOTE 6 – Exceptionally, terminals providing one or more wideband audio codecs, none of which are in the above list (e.g., existing/legacy terminals), are recommended to be permitted in NGN. Such terminals can optionally experience limited wideband audio interoperability.

14.2.3.3 Wideband audio codecs in networks

Network equipment originating and terminating end-to-end NGN IP media flows, supporting wideband audio is recommended to provide the following wideband audio codecs:

– ITU-T G.722 [ITU-T G.722];

NOTE 1 – To support DECT NG user equipment, some VoIP and/or legacy user equipment and/or interworking to other networks.

– AMR-WB/ITU-T G.722.2 [ITU-T G.722.2];

NOTE 2 – To support 3GPP user equipment, user equipment with mobility according to 3GPP access and/or interworking to 3GPP networks.

– ITU-T G.729.1 [ITU-T G.729.1];

NOTE 3 – Where required to support DECT NG user equipment, VoIP and/or legacy user equipment and/or interworking to some VoIP and legacy networks.

– EVRC-WB [TIA-127-C].

NOTE 4 – Where required to support 3GPP2 user equipment, user equipment with mobility according to 3GPP2 access and/or interworking to 3GPP2 networks.

14.2.4 Video codecs

In order to enable the interworking for video communication services between NGN and other networks, the support of the ITU-T H.263 profile 0 [ITU-T H.263] and ITU-T H.264 baseline profile [ITU-T H.264] codecs is recommended.

NOTE – The above does not make any requirement about the video codecs to be supported by terminals, nor does it mandate that NGN is required to support video transcoding between any arbitrary codec and ITU-T H.263 or ITU-T H.264-based codecs.

15 Content management

NGN is recommended to provide content management capabilities to manage various and huge content resources.

NOTE 1 – Objects of content management are typically classified as enterprise content (e.g., business documents); web services content (e.g., HTML files, images); IPTV services content (e.g., relatively large-size stream data). Content management in NGN provides the ability to manage the content life cycle (e.g., from creation through editing, approval, publishing and maintenance to archiving). In addition, content management provides the ability to support B2B processes between organizations according to their contractions.

NOTE 2 – As to IPTV services, detailed requirements of content management are contained in clause 14.1.

NOTE 3 – The content management capabilities involve, but are not limited, to:

– Content acquisition, aggregation and import of content/metadata from multiple external sources.

– Content/metadata format validation and verification as well as definition of the relationship between Content and its metadata.

– Content classification based on various classification standards.

– Content and metadata manipulation (e.g., adding, modifying, searching, copyright processing, adaptation).

NOTE 4 – Content adaptation includes the ability of content transformation in order to adjust to device capabilities and/or network constraints.

– Content dispatching within NGN according to assignment of content delivery resource, content publishing restriction, and so on.

– Content monitoring and auditing (e.g., monitoring of content state and/or content manipulation result, content analysis and statistics).

16 Operations and provisioning

16.1 Requirements for NNA (numbering, naming and addressing)

NGN is intended to provide an efficient, secure and trustworthy numbering, naming and addressing environment for users, network operators and service providers. Regulatory requirements as well as interoperability with PSTN/ISDN will be taken into account where applicable.

Evolution to NGN is required to ensure that the sovereignty of ITU Member States with regard to the numbering plan, naming plan and addressing plans is fully maintained, in particular as described in [ITU-T E.164] and other relevant Recommendations and specifications of other standard bodies.

The following are the requirements to support numbering, naming and addressing capabilities. Except where noted, they apply to both the transport and service strata.

1) Both dynamic and fixed address assignment modes are required to be supported.
2) Numbering, addressing and naming capabilities can optionally be implemented by using an individual mapping scheme for each service, or via a mapping scheme that is common across different services.
3) Dynamic update of the naming databases is required to be supported (for example, in case of a mobile terminal, addresses at one or more layers may dynamically change depending on the terminal's location).

NOTE – These repositories could be ITU-T X.500 directories accessed as specified in [b-ITU-T X.511]

16.1.1 Numbering

The numbering requirements applicable to NGN are the following:

1) Addressing mechanisms are required to support the ability to differentiate between the dialling plan, numbering and addressing plans.
2) Addressing mechanisms are required to support the ability to translate a dialling sequence into the numbering and addressing scheme.
3) NGN is required to support ITU-T E.164 numbering (global numbers).
4) NGN is recommended to allow non-ITU-T E.164 numbering (local numbers).
5) NGN is recommended to allow short numbers in national dialling plans.
6) NGN is not recommended to prevent private and corporate numbering (see clause 17).
7) When non-ITU-T E.164 numbers (local numbers) or dialling sequences are used, NGN addressing is required to provide the scope within which the local numbers are valid.
8) NGN is required to support international ITU-T E.164 numbering.
9) NGN is required to support national ITU-T E.164 numbering.
10) NGN is required to support short codes (non-ITU-T E.164 numbers) in national dialling plans.
11) NGN is required to support private numbering (e.g., service-specific and corporate numbering) (see clauses 17.1 and 17.2).
12) When national ITU-T E.164 numbers or short codes or private numbers are used, NGN addressing is required to provide the scope within which these numbers are valid.
13) NGN is required to support the ability to differentiate alphanumerical identifiers that happen to consist of only digits from those which are telephone numbers, and is recommended to be treated as such in routing procedures.

16.1.2 NNA schemes

1) At the transport stratum, NGN is required to support IP addressing schemes based on IPv4 or IPv6 or both.

   NOTE 1 – It is recommended to be recognized that a mixture of IPv4 and IPv6 within a single domain may cause problems for service delivery.

2) NGN domains can optionally support user equipment using IPv4 only, IPv6 only or both at the user-to-network interface.

   NOTE 2 – It is assumed that IPv6-based user equipment can also support IPv4 at the user-to-network interface.

3) NGN is required to support IP multimedia communication establishment (in both the originating and terminating case) using at least ITU-T E.164 telephone uniform resource identifiers (Tel URIs), e.g., tel: +4412345678, and SIP uniform resource identifiers (SIP URIs), e.g., sip:my.name@company.org, as a minimum. For Tel URIs:

   – international ITU-T E.164 numbers are required to be supported;

   – national ITU-T E.164 number form and short code support is required.

4) In some service scenarios, e.g., interworking with PSTN/ISDN, an NGN is required to support IP multimedia communication establishment (in both the originating and terminating case) using ITU-T E.164 numbering with ENUM-like support where appropriate.

5) Numbering and addressing schemes are required to support unicast and multicast service types.

6) Numbering and addressing schemes is recommended to support broadcast service types.

7) Other numbering, naming and addressing schemes can optionally be supported.

   NOTE 3 – Other numbering, naming and addressing schemes, such as distinguished names as specified in [b-ITU-T X.501], are for further study. .

16.1.3 NNA resolution

[ITU-T Y.2001] provides fundamental principles and requirements for name, number and address resolution. In line with those, the following requirements are provided.

1) Scalability: NGN is recommended to be scalable in order to handle increased demand for name/number/address resolution.

2) Reliability: Name/number/address resolution capabilities are required to remain unaffected by a single point of failure (using, for example, distributed resolution mechanisms).

3) Security: Security measures are required to be in place for name/number/address resolution capabilities.

   NOTE – These capabilities can optionally use databases supporting directory services that are internal or external to an NGN (e.g., an Internet DNS database, LDAP [b-ITU-T X.511]). Examples of security measures include user access authentication, data security, data synchronization and fault recovery.

16.1.4 NNA interworking

The interworking functions perform translations of numbers, names and addresses when required in network interconnection scenarios.

1) NGN is required to support multiple transport stratum address interworking scenarios minimizing influence upon the service provided to users (i.e., interworking scenarios among different addressing domains, such as domains based on IPv4 or IPv6 addressing schemes, and domains based on public or private addressing schemes).

2) Where needed, address translation capabilities are required to be used to support address format differences, in both the transport and service strata, minimizing the influence upon the service provided to users.

16.2 Accounting and charging

Accounting and charging capabilities are supported in NGN in order to provide accounting and charging data to the network operator regarding the utilization of resources in the network.

NGN requirements for accounting and charging are summarized below:

1) Accounting and charging capabilities are required to support the collection of data for later processing (offline charging) as well as near-real time interactions with applications such as those for pre-paid services (online charging).

2) Open mechanisms are required to be available for charging management.

3) Various charging policies are required to be supported (e.g., fixed rate charging and usage-based per-session charging).

4) Accounting and charging capabilities are required to support services with multicast functionality.

5) NGN is required to enable all possible types of accounting arrangements, including transfer of accounting/charging information between providers. This requirement also includes e-commerce arrangements.

   For example, in content delivery services scenarios with multicast functionality, services may be provided by joint activities of multiple companies (e.g., several content service providers and a network provider): charging functionality between companies is necessary in addition to charging functionality to users.

6) NGN is required to support interfaces and protocols between network elements and accounting elements and between accounting and charging elements to collect and transport resource usage data (e.g., accounting metrics and charging information records (CIRs)). These interfaces and protocols are required to comply with [ITU-T Y.2233].

7) NGN is required to support management functionalities for the seamless operation of the accounting and charging functional elements [ITU-T Y.2233].

8) NGN is recommended to support flow-based accounting and charging functionality for various NGN services (e.g., unidirectional flow resource usage, bidirectional flow resource usage, session resource usage). Such functionality must be accurate, reliable and scalable.

NOTE – The usage of charging information collected by an NGN to enable billing arrangements is out of scope of this Recommendation.

16.3 OAM requirements

It is recognized that OAM capabilities are important in public networks for ease of network operation, for verifying network performance, and to reduce operational costs by minimizing service interruptions, service degradation and operational downtimes. OAM capabilities are especially important for networks that are required to deliver (and hence be measurable against) network performance and availability objectives [ITU-T Y.1710], [ITU-T Y.1730].

NGN is required to provide OAM functions for both service and transport strata.

In order to offer reliable NGN services that can support the requirements of SLAs, NGN services are required to have their own OAM capabilities.

NOTE 1 – The OAM capabilities described in this clause are complementary to the management capabilities described in clause 11.

The following provides OAM requirements of NGN:

1) The capability to choose the desired OAM functions by the service or network provider is required to be supported.
2) OAM functions are required to be applicable to point-to-point, point-to-multipoint and multipoint-to-multipoint applications.
3) OAM functions are required to allow efficient scaling to large network sizes.
4) The capability to support detection of faults, defects and failures is required to be supported.
5) The capability to diagnose, localize and notify the network management entities and take appropriate corrective actions is required to be supported.
6) The capability to allow NGN to prevent the customer from triggering any service/network provider OAM function is required to be supported.
7) The capability to allow NGN to prevent the customer from detecting or localizing failures (since this is part of service provider or network provider's responsibility) is required to be supported.
8) OAM traffic is required to follow the same path as the user traffic.
9) The following anomalies are required to be automatically detected:
   - lost data;
   - loss of connectivity;
   - errored data;
   - unintentionally self-replicated data;
   - misinserted data [ITU-T Y.1730].
10) OAM functions are required to be backward compatible. NGN is required to be capable of activating OAM functions transparently without disturbing the user traffic or causing unnecessary actions.
11) OAM functions are required to perform reliably even under degraded transmission conditions, e.g., error events.
12) Connectivity status assessment is required to be independent of the dynamic behaviour of user traffic [ITU-T Y.1710], [ITU-T Y.1730].
13) Server-client layer OAM relationships between lower layers and higher layers (e.g., signal fail/signal degrade) in case of a multi-layer network is required to be supported.
14) In case of a multi-layer network, a defect event in a given server layer network is required to avoid causing multiple alarm events to be raised, and is required to avoid unnecessary corrective actions to be taken, in any higher client layer network. Client layer networks are recommended to support alarm suppression for server layer sourced defects whose presence has been communicated by forward defect indication means. Client layer networks are required to support forward defect indication capability [ITU-T Y.1710], [ITU-T Y.1730].
15) In case of a multi-layer network, OAM functions in a given layer network are required to be independent of any specific lower or higher layer network. This is architecturally critical to ensure that layer networks can evolve, be added and removed without impacting other layer networks.
16) In case of a multi-layer network, OAM functions in a given layer network are required to be sufficiently independent of any specific control plane such that control plane changes do not impose changes in user plane OAM. This is architecturally critical to ensure that user plane and control plane can evolve without impacting each other.

17) OAM functions are required to be supported in multiple service/network provider environments.

18) When NGN services are provided in multiple service/network provider environments, it is required to detect and notify which service/network provider is responsible for the defect so that quick action can be taken. Additionally, the service/network provider that offers the service to the user is required to be made aware of the service fault, even if the fault and detection point are located in the network of another service/network provider.

19) NGN is required to have mechanisms that make sure that service/network providers' OAM flows, which are meant for their internal use, are confined within their networks and do not leak out to customers or other service/network providers.

20) In order to realize OAM functions in hybrid networks, so that services can be provided across an end-to-end path comprising a combination of NGN and non-NGN networks, OAM functions are required to be supported in interworking scenarios (clause 18.3).

21) In order to allow separate management of a portion of a network which is under the responsibility of a provider, and to allow the flexible definition of maintenance entities, both "segment" OAM functions and "end-to-end" OAM functions are required to be supported.

NOTE 2 – Segment means a part of an end-to-end connection which is defined for operation and maintenance purposes.

22) Recording of service downtime for performance and availability measurements is required to be supported.

23) The information produced by OAM functions is required to be managed so as to provide the appropriate indications to the maintenance staff for maintaining the quality of service level offered to customers [ITU-T I.610].

24) Capabilities for performance monitoring are required to be supported.

16.4 Policy management

Policy management may be used in NGN to:

1) Ensure service consistency across a range of access and core network technologies. This can be also applied across multiple service provider networks.

NOTE 1 – The policy applied to each network depends on the network technologies and it may be specific to each network technology.

2) Provide admission control with respect to usage of network capabilities and network resources by services and applications.

3) Provide network resource usage logging.

NOTE 2 – This can be viewed as the function that produces information which may be used by other network capabilities, such as accounting and charging functions.

4) Shield services and applications from the intricate details of transport network implementation.

NOTE 3 – Policy control can be used to serve the needs of applications, while remaining agnostic about the network technologies deployed.

With the basic areas of applicability indicated above, and policy operating in conjunction with connectivity QoS and security, many actions can be taken in the policy management space that can benefit NGN services. For example, policy management may be applied to:

– service provisioning;

– service configuration;

– authorization (i.e., entitlements);

– service delivery;

– accounting and charging.

Policy management can invoke policy rules to provide reliable, consistent, deterministic outcomes called policy decisions. The complexity of these rules will be a function of their intended use.

NOTE 4 – QoS management capabilities such as resource and admission control (clause 9) may be seen as part of the global policy management capability set.

NGN policy management general requirements are as follows:

1) Policy management capabilities are required to be supported in order to ensure service access, provisioning and management.

2) Policy management capabilities are required to work within specific services, and within specific provider domains or across multiple provider domains.

3) Policy management capabilities are required to refuse or not respond to unauthorized requests, and respond to authorized requests.

16.5 Survivability requirements

Survivability functions are necessary to realize highly reliable networks.

16.5.1 Protection switching

NGN is required to support protection switching capabilities to implement fast and deterministic survivability functions for all traffic paths.

The following are general requirements for NGN transport protection switching:

1) Capabilities to prevent a higher layer defect from triggering lower layer protection switching are required to be supported.

2) When more than one layer is involved in protection switching, the lower layers are required to have priority over the higher layers (this is known as inter-layer escalation strategy).

3) Both 1+1 and 1:n protection switching is recommended to be provided.

4) Unutilized transport protection resources can optionally be used to carry best effort traffic.

5) Impacts on network performance (e.g., additional delay, delay variation, bit errors, packet losses, etc.) due to protection switching are recommended to be minimized.

6) Operator control functions, such as lockout of protection, forced switch and manual switch commands, are required to be supported.

Detailed requirements for specific technologies are provided in various Recommendations such as [ITU-T G.808.1].

16.5.2 Rerouting

When serious accidents or special events occur, network degradation or, in the worst case, failure may occur. Capabilities such as rerouting, with possible downgrading of performance or quality of service, and traffic control mechanisms are therefore required.

NOTE – These capabilities can also be regarded as part of network integrity functions.

General requirements for NGN rerouting are as follows:

1) When more than one layer is involved in rerouting, the lower layers can optionally have priority over the higher layers (inter-layer escalation strategy).

2) The rerouting mechanism is required to be capable of finding an alternative route within an acceptable time.

3) Impacts on network performance (e.g., additional delay, delay variation, bit errors, packet losses, etc.) due to rerouting are recommended to be minimized.

4) NGN is required not to preclude operator control.

5) Network re-optimization is required to be supported, where necessary, after restoration of the impaired traffic.

6) After recovery from fault or degraded conditions, the performance and quality of service levels preceding the fault or degraded conditions are required to be restored.

16.5.3 Service resiliency

Resiliency conditions depend on the specific service; therefore, they are required to be described for each service as required.

General requirements for service resiliency (SR) are as follows:

1) NGN is required to be able to independently assign different SR levels to different services.

2) NGN is required to be able to independently assign different SR levels to different services on a per-flow basis.

3) Depending on the assigned SR level, NGN is required to support the capability for the services covered by SR to experience the same level of service quality experienced prior to the failure event.

4) Terminal equipment can optionally signal SR levels to NGN.

5) NGN is required to be able to assign and support SR from the point of ingress to the point of egress of the service provider network.

6) NGN is required to be able to differentiate among user plane and control plane SR-enabled flows.

7) NGN is required to support the capability to notify the application/user if the required SR level cannot be met by NGN.

17 User networks including enterprise networks

17.1 General requirements on NGN for access via user networks

The following are general requirements on NGN for access via user networks:

1) NGN is required not to preclude solutions for access via a user network to an NGN with NAT/NAPT and firewalls in the user environment where the assignment of IP addresses to user equipment may be done by the user network. These addresses need not be routable in the NGN.

2) Solutions for access via a user network to an NGN are required to have minimal impact on existing user network deployments.

3) Solutions for access via a user network to an NGN are required to support the following configurations:

   – direct connectivity and interaction between the individual terminals and the NGN;

   – indirect connectivity and interaction between the individual terminals and the NGN (via home networks and enterprise networks).

NGN is recommended to allow the simultaneous use of multiple types of access transport functions by a single terminal; however, there is no requirement to coordinate the communication. Such terminals may therefore appear to be two or more distinct terminals from the network point of view.

NOTE – It is not intended to preclude the attachment of terminal equipment which could enable interface adaptation to varying user requirements, including the needs of people with disabilities, using commonly provided user interface devices.

17.2 General requirements for user networks

The high-level requirements for user networks connected to NGN are as follows:

– User networks connected to NGN are recommended to enable user access:
  1) to services provided by NGN;
  2) to services provided within user networks themselves (locally and through interconnected NGN);
  3) as enterprise and home user.

– User networks connected to NGN are recommended to support:
  1) security, management and QoS for home networks;
  2) device provisioning and service configuration (user terminals, user network gateways), including remote access.

17.3 Enterprise networks

17.3.1 Introduction

This clause specifies high-level requirements for enterprise communications in order to:

1) support connection and interoperation of enterprise communication capabilities (either hosted in a next generation corporate network (NGCN) or NGN) to NGN;
2) support connection and interoperation of enterprise communication capabilities to other enterprise communication capabilities (either hosted in NGCN or NGN);
3) support connection and interoperation of enterprise communication capabilities to other enterprise communication capabilities located in or connected to the ISDN and PSTN;
4) support hosted enterprise services in an NGN.

NOTE 1 – This Recommendation specifies network requirements to support connection of NGCN directly to an NGN as well as network requirements for communication between NGCN capabilities (including user equipment) to other NGCN capabilities of the same enterprise through NGN (e.g., geographically separated).

NOTE 2 – It is assumed that existing legacy service requirements apply in the case of attachment of legacy PBXs to NGN.

17.3.2 Types of enterprise traffic

The traffic generated or received on behalf of an NGCN can be either:

– Traffic sent to the NGN for processing according to normal rules of the NGN. This type of traffic is known as public network traffic.

– Traffic sent to the NGN for processing according to an agreed set of rules specific to an enterprise. This type of traffic is known as private network traffic. Private network traffic is normally sent within a single enterprise, but private network traffic can also exist between two different enterprises if not precluded for regulatory reasons.

  NOTE – An enterprise network can optionally separately distinguish private network communications that originate in the NGN from private network communications that originate in the enterprise: this is out of scope of this Recommendation.

NGN is required to distinguish public network traffic from private network traffic.

NGN is required to distinguish private network traffic belonging to one enterprise from that belonging to another enterprise.

Private network traffic can optionally require different handling in the NGN compared to public network traffic.

Except where national regulations and laws do not permit, NGN is required to treat traffic between enterprises as public network traffic. In such cases, as part of the capabilities provided to the enterprise, NGN can optionally provide break-out and/or break-in capabilities on behalf of each enterprise.

For private network traffic, NGN is required to be transparent to signalling mechanisms, except where there is a specific need for NGN to intervene in order to deliver the service requested by enterprise customers.

17.3.3 Enterprise communication capabilities

NGN is required to allow the use of any IP-based media during an enterprise communication subject to the availability of resources and contractual arrangements.

Except where authorized through explicit agreement with the NGCN (by signalling or contract), or to meet formal legal requirements, NGN is required to not intervene in the media which is transported in NGN.

NOTE 1 – Examples of reasons for agreed intervention are transcoding, translation and bridging. The default of no intervention is to avoid undue performance impairment (particularly for real-time telemetry data, bidirectional audio and video) and to safeguard perceived confidentiality of the media.

NGN is recommended to allow the transport of signalling itself while the transport of media is performed via other networks.

NOTE 2 – For example, for communication between two enterprise networks, NGN may be involved in signalling (to assist in routing from the first enterprise to the second enterprise), but media traffic may flow directly through other IP networks.

NGN can optionally provide the following capabilities to an enterprise:

a) Virtual leased line, where NGCN sites are interconnected through the NGN. No additional capabilities are provided by the NGN.

b) Business trunking application, where the NGN hosts transit capabilities between NGCNs, break-in capabilities from NGN to NGCN and break-out capabilities from NGCN to NGN. A business trunking application can optionally also host additional capabilities beyond basic break-in, break-out and transit capabilities to the NGCN. Typically, there is no corporate network terminal equipment connected directly to an NGN.

c) Hosted enterprise services (HESs), where an NGN hosts originating and/or terminating enterprise communication capabilities for enterprise communication users that are directly attached to an NGN and have a subscription for these services in this NGN.

17.3.4 Location management

NGN is required to provide the geographical location information of an NGCN user to an NGCN. This can be subject to privacy requirements.

NOTE 1 – An NGCN can use the geographical location information, for example, to provide location-based services to the NGCN user.

NOTE 2 – The source of geographical location information may be an NGN or an NGCN user.

17.3.5 Signalling

NGN is required to offer one standardized signalling for interfacing with an NGCN.

17.3.6 Routing

17.3.6.1 Routing to an NGCN user

NGN is required to support routing to NGCN users that do not have an NGN service subscription, but can be reached through an NGCN site that has a business trunking arrangement with an NGN.

NOTE – In this case, an NGCN site has an NGN service subscription, the corporate network users in an NGCN do not need their own NGN service subscription, since they are owned and managed by the NGCN. What this requirement achieves is that these corporate network users can be reached from the public part of the NGN by addressing them directly using a public address.

17.3.6.2 Number range-based routing

To be able to route to corporate network users in an NGCN, NGN is recommended to support routing only on a specific [ITU-T E.164] number range that is assigned to this NGCN.

17.3.7 QoS control

NGN is required to support communication admission control on a per-NGCN site basis.

NOTE 1 – The NGN provider defines the set of rules or policies under which this is recommended to occur, and the NGCN provider is recommended to be able to configure the capability within those rules and policies.

It is required to allow the setting of the following thresholds on a per-direction basis (i.e., incoming and outgoing communications):

1) maximum number of simultaneous session-oriented communications;

2) maximum number of simultaneous streams per communication.

Communications coming in excess to the allowed threshold may be accepted or rejected.

NOTE 2 – The enterprise may select values for communication admission control that correspond to the service level agreement (SLA) between the enterprise and the NGN provider. If this occurs, then communications coming in excess of the allowed threshold which are accepted may be subject to specific charging rules.

17.3.8 Identification

17.3.8.1 NGCN site identification

NGN is required to support identification of an NGCN site, for authentication and authorization purposes.

NOTE 1 – The NGCN site identification is needed to be able to let the NGN determine which NGCN site a communication is originating from.

NOTE 2 – An NGCN can optionally have more than one NGCN site, and hence more than one NGCN site identifier, associated.

17.3.8.2 Enterprise network user identification

In addition to the naming, numbering and addressing requirements in clause 16, NGN is required to provide the capability to uniquely identify NGCN users. NGCN user identifiers are assigned by an NGCN.

NOTE 1 – This does not exclude scenarios where one organization acting as an NGN provider also in another role administers the NGCN of an enterprise on behalf of that enterprise.

NOTE 2 – The above requirement ensures that, for communications from an NGCN user to an NGN user, the NGN user's (originating identity presentation (OIP)) service can present the correct identifier of the calling NGCN user.

NOTE 3 – The above requirement ensures that, for communications from an NGN user to an NGCN user, the NGN user's (termination identity presentation (TIP)) service can present the correct identifier of the called NGCN user.

NOTE 4 – The above requirement ensures that NGN users can call NGCN users that have identifiers within the set of identifiers that are available to that NGCN under the business trunking arrangement for that NGCN.

NGN is not recommended to prevent an NGCN to assign new user identifiers within its domain without prior arrangement with the NGN.

NGN is recommended to support NGCN user identifiers that map to ITU-T E.164 numbers.

NGN is not recommended to prevent an NGCN to change mappings between user identifiers within its domain and ITU-T E.164 numbers without prior arrangement with the NGN.

NOTE 5 – This implies that for a communication from PSTN/ISDN to the NGCN, the NGN should be able to determine that the called ITU-T E.164 number is within the NGCN domain and hence route the communication to the NGCN indicating as destination either the called ITU-T E.164 number or a discovered NGCN identifier obtained from information published by the NGCN (e.g., DNS).

NGN is recommended to support NGCN user identifiers that do not map to ITU-T E.164 numbers.

NOTE 6 – Although NGCN user identifiers that do not map to ITU-T E.164 numbers will not be directly reachable from PSTN/ISDN, they should be reachable by other NGCN or NGN users.

NGN is not recommended to prevent from delivering of calling and connected user identifiers to the NGCN, subject to availability and the absence of privacy or regulatory requirements that forbid such delivery.

NGN is not recommended to prevent application of privacy to calling and connected user identifiers within an NGCN on a permanent or communication-by-communication basis, such that identifiers are not disclosed to other parties.

NOTE 7 – This means that an NGN must not deliver to other parties in such circumstances either an identifier supplied by the NGCN (and marked as private) or a default identifier that NGN assigns to the NGCN.

17.3.9 Authentication

Authentication with regard to connection of an NGCN to NGN is required to comply with requirements specified in this clause and clause 10.3.

17.3.10 Security

Security with regard to connection of an NGCN to NGN is required to comply with the requirements specified in clause 10.

17.3.11 Mobility management

This clause specifies requirements for roaming in the context of enterprise communications.

For roaming in the context of enterprise communications, nomadism for both terminal mobility and personal mobility is recommended to be supported.

In particular, it is recommended that an NGCN user be able to register and receive service from their NGCN while roaming to:

a) another NGCN site of the same NGCN and interconnected by NGN;

b) NGN to which the NGCN is directly connected;

c) NGN to which the NGCN is indirectly connected via another NGN.

Over and above the roaming capabilities provided for NGN users in this clause, it is recommended that, subject to agreement with the NGCN, an NGN user be able to register and receive service from their NGN while roaming to:

a) an NGCN connected to the NGN;

b) an NGCN indirectly connected to the NGN.

17.3.12 Accounting

An enterprise can account for traffic in its enterprise communication capabilities whether hosted in an NGCN or NGN.

For public network traffic, the requirements in [ITU-T Y.2201] and [ITU-T Y.2233] apply.

For public network traffic, the enterprise and the NGN provider are required to be able to identify each other across any interconnection interface, including intra-NGN interfaces to hosted enterprise communication capabilities.

For private network traffic, any involved enterprise is required to be able to identify each other across any interconnection interface between its enterprise communication capabilities.

Any enterprise communication capability hosted in an NGN is required to be able to account for private network traffic to the enterprise in the same manner as for an NGN provider to account for its own traffic.

Additionally, for private network traffic, the enterprise and the NGN provider are required to be able to identify each other across any interconnection interface.

18 Interconnection and interworking

Interoperability and interworking are two distinct functions and are defined respectively in [ITU-T Y.101] and in the ITU-T Y.1400-series Recommendations.

18.1 Interconnection requirements

Two types of interconnection between NGNs are distinguished:

– "connectivity-oriented interconnection": It is based on simple IP connectivity irrespective of the levels of interoperability;

NOTE 1 – An interconnection of this type is not aware of the specific end-to-end service and, as a consequence, network performance, QoS and security requirements specific to the service are not necessarily assured.

– "service-oriented interconnection": It allows carriers and service providers to offer services with defined levels of interoperability.

NOTE 2 – For example, this is the case for ITU-T G.711 services over IP interconnection. The defined levels of interoperability are dependent upon the service or QoS or security, etc.

NOTE 3 – Only service-oriented interconnection fully satisfies NGN interoperability requirements.

The requirements for interconnection are the following:

1) Connectivity-oriented interconnection type between NGNs is required to be supported.

   It is required to support this type of interconnection between NGNs using different versions of IP.

2) Service-oriented interconnection type between NGNs is required to be supported.

   It is required to support this type of interconnection between NGNs using different versions of IP.

3) Service-oriented interconnection between NGN and NGCN is required to be supported, when NGN provides hosted enterprise services.

   It is required to support this type of interconnection between NGN and NGCN using different versions of IP.

18.1.1 Service-oriented interconnection between IMS-based NGNs

The requirements for service-oriented interconnection between IMS-based NGNs are the following:

1) The interconnection logical link between NGN providers is required to be "aware" of specific NGN services. It may be a physical or a logical link which carries both data and signalling bearers. NGN is required to offer one standardized interface of interconnection with another NGN.

2) It is required to control the resources on the interconnection link in order to deal with data and signalling bearer characteristics of different services.

3) Security and accounting features are required to be taken into account.

Other detailed requirements for service-oriented interconnection are for further study (e.g., in the areas of signalling, codec, routing, security, charging and accounting, resource, QoS and SLA).

18.2 Interoperability requirements

In order to enable certain services to be provided across an end-to-end path comprising a single NGN domain or multiple NGN domains:

1) appropriate service components within a single NGN domain are required to interoperate;

2) interoperability of interconnected NGN domains which deploy identical sets of service capabilities is not precluded.

18.3 Interworking requirements

NGN is required to interwork with various kinds of networks for provision of certain services. Services identified for interworking are required to operate seamlessly across the infrastructure provided by one or more network providers. NGN provides capabilities, including, among others, security, OAM, resiliency, quality of service and, where needed, media transcoding, for support of interconnection scenarios with other non-NGN networks in order to ensure seamless end-to-end operations.

In order to enable certain services to be provided across an end-to-end path comprising a combination of NGN and non-NGN networks:

– NGN is required to be able to interwork with other non-NGN networks;

– NGN is recommended to aim to support the following interworking capabilities:

  - routing;
  - signalling interworking;
  - numbering, naming and/or addressing interworking;
  - accounting and charging-related information exchange;
  - security interworking;
  - QoS interworking;
  - user and terminal profile information exchange;
  - media interworking;
  - management interworking;
  - policy management (e.g., according to inter-domain policies, some trusted domain internal information, including user-related information, may need to be hidden or removed from the information flow exchanged at the interface with another trusted or non-trusted domain), including resolution of differences in policy.

  NOTE – This does not imply that all services and/or service features can be interworked. These requirements may only apply to the interworking between certain specific (and most likely similar or identical) services and/or service features.

18.3.1 Interworking with PSTN/ISDN

When an NGN is connected to a PSTN/ISDN, it is required to support the following:

1) Interworking between PSTN/ISDN and PSTN/ISDN emulation services: Interworking is required to provide a high level of interoperability with the services in the PSTN/ISDN

being emulated. The degree to which service interoperability is provided is a matter for operators and, in some cases, national regulators.

2) Interworking between PSTN/ISDN and PSTN/ISDN simulation services: Interworking is required to support the interoperability of PSTN/ISDN simulation services with PSTN/ISDN supplementary services, although this interworking may result in a limited service capability.

3) Interworking between PSTN/ISDN and NGN IP multimedia services, although this interworking may result in a limited service capability.

NOTE 1 – This does not imply that all NGN services and/or service features can be interworked with PSTN/ISDN services and vice versa. These requirements may only apply to the interworking between certain specific (and most likely similar or identical) services and/or service features offered by both the NGN and the PSTN/ISDN.

NOTE 2 – Circuit-switched-based corporate networks are supported either by connection to the NGN via an existing PSTN/ISDN or, when PSTN/ISDN emulation is deployed, through an interworking gateway.

18.3.2 Interworking with other networks

1) NGN is required to provide the capability for direct interconnection for circuit-switched-based networks, including at least cable networks, broadcast networks and public land mobile networks. The requirements for interworking to all circuit-switched-based networks are the same as those for interworking to the PSTN/ISDN.

NGN is required to provide the capability for connectivity-oriented interconnection with non-NGN but IP-based networks.

NGN is required to provide the capability for connectivity-oriented interconnection with non-NGN but IP-based networks using different versions of IP.

NGN is required not to preclude the capability for service-oriented interconnection with non-NGN but IP-based networks.

If the interconnected network provides all of the interworking capabilities, as identified in clause 18.3, such network interconnections may be supported in a deployment. The characterization and functionality of non-NGN but IP-based networks are sufficiently diverse and abundant that it is not possible to provide firm requirements for interconnection.

2) NGN is required not to deliberately exclude the interconnection with non-NGN but IP-based networks.

NOTE – Security requirements are contained in clause 10.6.

18.4 Non-disclosure of information across NNI and ANI interfaces

Where required, e.g., by regulation, law, country or regional conditions, NGN is required to have capabilities to enable:

– prevention of disclosure of internal information or service users' information to other entities across NNI interfaces;

– prevention of disclosure of internal network information as well as network users' information to other entities across NNI interfaces;

– prevention of disclosure of internal information or service users' information to other entities across ANI interfaces;

– prevention of disclosure of internal network information as well as network users' information to other entities across ANI interfaces.

18.5 Inter-provider exchange of user-related information

Where required, e.g., by regulation or law, NGN is required to support mechanisms to exchange user-related information between NGNs for service interoperability.

19 Service-specific requirements

19.1 PSTN/ISDN emulation

Evolution of networks to NGN is dependent on providers' choices and their needs. Network providers may choose an evolution path depending on their actual resources, business plans and strategies. Therefore, they may choose different technologies and time-frames.

For the transition period from PSTN/ISDN to NGN, NGN is required to provide the following capabilities:

1) PSTN/ISDN emulation capabilities;
2) PSTN/ISDN simulation capabilities.

Requirements for these capabilities are described below.

19.1.1 General

NGN is required to provide at least one level of service of PSTN/ISDN emulation that offers capabilities that are the same or better than those provided by circuit-switched networks.

19.1.2 Terminal

NGN is required to support legacy terminals (e.g., traditional PSTN phones, text phones, facsimile machines and other types of existing PSTN/ISDN terminals), which are not attached via an NGN UNI but via a PSTN/ISDN-like UNI.

NOTE – Emulation of the full PSTN/ISDN service set may not be possible and service support may be restricted to certain terminal types, i.e., legacy terminals or user equipment that behave like legacy terminals.

19.1.3 Service

Service requirements for PSTN/ISDN emulation are the following:

1) NGN is required to support the ability for service providers to emulate one or more of their PSTN/ISDN services.
2) NGN is required to support capability definitions inherited from existing PSTN/ISDN specifications.

NOTE – A specific NGN deployment need not support all possible capabilities and interfaces which are present in PSTN/ISDN.

19.2 Real-time multimedia conversational services including PSTN/ISDN simulation

19.2.1 General

NGN is required to support PSTN/ISDN simulation services that provide the user with a PSTN/ISDN-like experience.

19.2.2 Terminal

NGN is required to support non-legacy terminals for PSTN/ISDN simulation services. It can optionally also support adaptation devices to allow legacy terminals to connect via adaptation devices to NGN (e.g., black phones, text phones and facsimile machines).

19.2.3 Service

Service requirements for PSTN/ISDN simulation are the following:

1) NGN is required to support PSTN/ISDN-like service capabilities using session control over IP interfaces and infrastructure.

2) NGN is recommended to provide the ability for a service provider to simulate PSTN/ISDN services.

3) NGN is not required to provide services identical to those in PSTN/ISDN.

NOTE – It is assumed that the PSTN/ISDN simulation services do not utilize PSTN/ISDN call models or signalling protocols.

19.3 IPTV services

When NGN provides IPTV services, the following description applies.

Concerning the NGN requirements to support IPTV services, this Recommendation includes high-level requirements.

In order that IPTV services are supported by NGN, NGN capabilities in principle support the requirements described in [ITU-T Y.1901] in the context of replacing "the IPTV architecture" text with "the NGN environment" text inside the [ITU-T Y.1901] requirements. Specific considerations, such as which specific NGN capabilities support the requirements identified in [ITU-T Y.1901] and whether these are equally applied to all IPTV services or applications, need further study.

19.3.1 Service offering

The NGN architecture is required to support mechanisms for IPTV on-demand services (including push VoD [ITU-T Y.1901]), retransmission broadcast services [ITU-T Y.1901] (including linear TV [ITU-T Y.1901]), and interactive services. The NGN architecture is recommended to support mechanisms for cPVR [ITU-T Y.1901] and nPVR [ITU-T Y.1901]. The support of trick mode functionality [ITU-T Y.1901] is recommended for implementing some IPTV services.

The NGN architecture is recommended to support mechanisms by which end-users can make content they produced/created available to other end-users.

The NGN architecture is required to support the end-user with the ability to choose a preferred language option (audio, subtitles [ITU-T Y.1901], captions [ITU-T Y.1901], supplementary contents [ITU-T Y.1901] and audio descriptions [ITU-T Y.1901]) in various languages that the content provider predefined and the service provider delivered.

NOTE – Further information regarding "on-demand services" can be found in [b-ITU-T Y-Sup.5].

19.3.2 Transport and mobility

For support of IPTV services, the transport requirements in clause 6 including multicast support are applicable.

For support of IPTV services, the mobility handling requirements in clause 12 are applicable.

19.3.3 Service enablers

The NGN architecture is required to support discovery and selection capabilities, as well as navigation capability for IPTV content and services.

The NGN architecture is recommended to support viewership data tracking while protecting the user's privacy as required.

The NGN architecture is recommended to allow content usage statistics to be collected and content tracing.

The NGN architecture is recommended to have a means to allow content to be seen only by the appropriate audience according to specified geographical areas, parental rating and specified grouping. In particular, the NGN architecture is required to support mechanisms to block transmission of content to specified geographical areas whenever blackout requirements are applicable.

19.3.4 Middleware and metadata

The NGN architecture is required not to preclude any use of middleware and metadata specified for IPTV services.

19.3.5 QoS

Networks that support IPTV are required to support IP QoS classes and to satisfy associated performance requirements specified in [ITU-T Y.1541]. This includes maintaining accurate time-based control for synchronization, e.g., lip-sync. The NGN architecture is recommended to support means to provide channel changing times [ITU-T Y.1901] with sufficient quality of experience (QoE).

The NGN is required to support a framework that identifies the components and measurement points (including the end-user device) for quality of service measurement (QoSM).

19.3.6 Security

The NGN architecture is required to support service and content protection.

19.3.7 Management

The NGN architecture is recommended to support (remote) software upgrade and download for IPTV devices.

19.3.8 Media

The NGN architecture is required not to preclude any use of video and audio formats (including video resolutions, video aspect ratios, audio sampling rates and audio bit-depths) specified for IPTV services.

The NGN architecture is required not to preclude any use of video and audio codecs specified for IPTV services.

Transcoding during the delivery of IPTV contents in the NGN architecture is required to be avoided wherever possible.

19.3.9 Charging

The NGN architecture is required to support mechanisms for the collection of data for accounting and reporting purposes, partner settlements and reconciliation of end-user usage, such as service subscriptions, purchases and transactions. This is to support charging options such as pay-per-view [ITU-T Y.1901].

19.3.10 Terminal aspects

A terminal device supporting IPTV services is required to have the ability to select, receive and render multiple audio, video and associated control information.

The NGN architecture is recommended to support such terminal capabilities and to capture those capabilities to adjust service provisioning.

19.3.11 Interworking

Requirements to support interworking of IPTV services are for further study.

19.3.12 Public interest

The NGN architecture is required to support terminal devices for IPTV services, which constantly listen for emergency alert notification (EAN) messages.

The NGN architecture is required to support the availability of accessibility features (captions, subtitles, descriptive audio and multiple video streams such as for sign language) and their synchronization with the main content when viewed in normal playback.

The NGN architecture is recommended to support transmission of video or data with sufficient quality for perception of sign language interpretation, including lip reading. This requires the transmission of a sufficient number of frames per second and sufficient spatial resolution to reproduce details of the signing person's hands, face, lips, eyes and body [b-ITU-T H-Sup.1].

19.4 Enterprise services

19.4.1 Virtual leased line service

No service-specific requirements are identified in this Recommendation.

19.4.2 Business trunking application

No service-specific requirements are identified in this Recommendation.

19.4.3 Hosted enterprise services

When NGN provides hosted enterprise services, NGN is required to:

– Support communications for enterprises that comprise both users supported by NGCN and users supported by HES, including communications between a user supported by NGCN and a user supported by HES.

– Allow an enterprise user to move between a location of an NGCN and a location supported by HES without the need for communication partners to be aware of that change.

– Allow an enterprise user to move his/her terminal between a location of an NGCN and a location supported by HES with minimal reconfiguration.

19.5 Applications and services using tag-based identification

When NGN provides applications and services using tag-based identification, [ITU-T Y.2213] specifies corresponding service-specific requirements.

19.6 Managed delivery services

When NGN provides managed delivery services, [ITU-T Y.2212] specifies corresponding service-specific requirements.

19.7 Visual surveillance services

A terminal-to-terminal visual surveillance service enables one terminal to receive and monitor multimedia information produced by other terminal (source) as well as remote control of the source device.

A server-to-terminal visual surveillance service enables multiple terminals to receive and monitor the same multimedia information produced by a single source server.

A terminal-to-server visual surveillance service enables one server to collect multiple pieces or an aggregated piece of multimedia information produced by multiple terminals (sources).

When NGN provides visual surveillance services, NGN is required to support:

– Terminal-to-terminal (including one-to-one and one-to-many) visual surveillance services (e.g., visual surveillance service for home security supervision).

– Server-to-terminal (including one-to-one and one-to-many) visual surveillance services (e.g., visual surveillance service for public traffic supervision).

Requirements for terminal-to-server visual surveillance services are for further study.

19.7.1 Server-to-terminal visual surveillance service

NGN is required to support discovery and selection capabilities, as well as navigation capability for server-to-terminal visual surveillance services.

NGN is recommended to allow content usage statistics to be collected and content tracing.

NGN is recommended to have a means to allow content to be seen only by the appropriate audience according to specified geographical areas, parental rating and specified grouping. In particular, NGN is required to support mechanisms to block transmission of content to specified geographical areas whenever blackout requirements are applicable.

NGN is required to support service and content protection.

NGN is recommended to support (remote) software upgrade and download for server-to-terminal visual surveillance devices.

19.7.2 Terminal-to-terminal visual surveillance service

For support of terminal-to-terminal visual surveillance services, NGN is required to support the requirements in the following subclauses.

19.7.2.1 Session handling

NGN is required to support session admission control with visual surveillance-related information.

NGN is required to support session handling with visual surveillance-related information (e.g., service-specific data such as remote control).

19.7.2.2 Routing

NGN is required to support routing based on originating and/or terminating terminal capabilities (e.g., media support).

19.7.2.3 Codecs

The NGN architecture is required to allow any use of video and audio codecs specified for visual surveillance services.

Transcoding during the delivery of visual surveillance information in the NGN architecture is required to be avoided wherever possible.

19.8 Ubiquitous sensor network (USN) applications and services

Service-specific requirements are for further study.

19.9 Multimedia communication centre services

Service-specific requirements are for further study.

19.10 VPN services in NGN

When NGN provides VPN services, [ITU-T Y.2215] specifies corresponding service-specific requirements.

20 Public interest aspects

NGN is required to provide capabilities for the support of public interest services required by regulations or laws of national or regional administrations and international treaties. These public interest services may include, among others, the services described in this clauses.

20.1 Lawful interception

1) An NGN transport provider and/or NGN service provider are required to respond to lawful interception requirements. Therefore, NGN is required to provide mechanisms that make lawful interception possible where required by regulation or law of a country in their application area.
2) The lawful interception mechanisms are required to provide access to content of communication (CC) and intercept related information (IRI) by law enforcement agencies (LEAs), as per the requirements of administrations and international treaties.

Because the nature of lawful interception is dependent upon national/regional customs and laws, requirements are dependent upon the regulatory environment of each country.

20.2 Malicious communication identification

NGN is required to include the capability to identify the source of a malicious communication, e.g., obtaining the identifier of the terminal involved or the location of the originator of the communication.

20.2.1 Malicious communication identification for enterprise

A communication identified as public network traffic is required to be handled in accordance with the malicious communication identification requirements of the NGN.

Identification of malicious communications in private network traffic is outside the scope of this Recommendation. NGN is required not to handle such communications. This also applies to a hosted NGCN capability.

NOTE – Separate regulatory requirements can apply for private network traffic.

20.3 Unsolicited communication

NGN is required to provide capabilities to prevent unsolicited communication (UC).

NGN is required to provide the ability to handle detected and marked communication attempts in order to react on them (e.g., redirecting the communication to a mailbox, voice-mailbox or junk-mail).

NGN is recommended to provide mechanisms to counter UC (e.g., black/white list, reputation system, address masking, content filtering).

NOTE 1 – For further information about these mechanisms, see [b-ITU-T X.1244].

NGN is recommended to provide a mechanism to allow UC reporting by NGN users.

NGN is recommended to provide a mechanism to audit UC reports made by NGN users.

NGN is recommended to:

- Provide the ability for a UC-affected user to request UC marking (rating).
- Provide the ability for a UC-affected user to correct UC marking.

NOTE 2 – For further information about UC rating, see [b-ETSI TS 187 009]

20.4 Emergency telecommunication

Emergency telecommunication (including support of early warning) include:

– individual-to-authority telecommunication, e.g., calls to emergency service providers;

– authority-to-authority telecommunication, e.g., telecommunication for disaster relief (TDR);

– authority-to-individual telecommunication, e.g., community notification services.

NOTE – In addition to being used for authority-to-authority telecommunication, TDR and emergency telecommunication service (ETS) may also be used for authority-to-individual telecommunications.

[ITU-T Y.1271], [ITU-T E.106] and [ITU-T E.107] provide "framework(s) on network requirements and capabilities to support emergency telecommunication over evolving circuit-switched and packet-switched networks", "international emergency preference scheme (IEPS) for disaster relief operations" and "emergency telecommunication service and interconnection framework for national implementations of ETS", respectively.

NGN is required to make network capabilities available to early warning applications, e.g., to provide geographical location information to support provision of warning messages only to those possibly affected by an impending disaster.

The support of emergency telecommunication and early warning requires the NGN to be operationally robust and have high availability.

NGN is required to:

1) Include service- and transport-level capabilities to allow emergency telecommunication to be supported using priority/preferential schemes. Call/session control of emergency telecommunication and emergency telecommunication bearer traffic is required to receive priority treatment during congestion/failure conditions.

2) Provide, as necessary, the interworking and mapping of priority mechanisms between the various components of NGN (e.g., between the access and the core network, and between the service stratum and the transport stratum) and between NGNs (e.g., between two core service provider networks) to assure appropriate end-to-end priority/preferential telecommunication.

3) Support existing telecommunication services, including an equivalent to all existing PSTN/ISDN emergency telecommunication services, even when one or more of the communicating entities are attached to an NGN and one or more are attached to a PSTN/ISDN.

4) Enable new emergency telecommunication means (e.g., instant messaging) to be supported in future deployments by authorities (such as emergency service providers).

5) Provide seamless interworking of emergency telecommunication across all public networks within an administrative (emergency) domain.

6) Provide routing of emergency telecommunication to appropriate authorities.

7) Provide routing of emergency telecommunication from the authority to individuals.

8) Provide, where possible, continuation of emergency telecommunication between the authority and individuals until the authority terminates the session, even though the individual may have hung up.

9) Provide to the authority information regarding the individual's geographical location as well as their identifier according to national or regional regulation requirements. When required by regulation or law, this information can be acquired by the authority even though the individual requested withholding this information.

10) Provide the ability for both authenticated and unauthenticated access to emergency telecommunication services according to national or regional regulation requirements. For example, NGN is required to provide the ability to authenticate user access to ETS/TDR telecommunication.

11) Support exemption of emergency telecommunication from certain restrictive network management functions.

12) Support emergency telecommunication with alternative and multiple media when required (e.g., by regulation or law). Video, text and voice and any combination thereof, as well as various forms of messaging, are essential for telecommunication with the emergency services for people with disabilities.

13) Provide capabilities to ensure that only authorized early warning messages are distributed.

14) Provide capabilities to prevent untargeted and unnecessary early warning-like messages.

20.4.1 Emergency telecommunication for enterprise

Both public network traffic and private network traffic can optionally carry emergency telecommunication for enterprise.

1) An emergency telecommunication for enterprise identified as public network traffic is required to be handled in accordance with the emergency telecommunication requirements of NGN.

2) In case of a public network traffic emergency telecommunication for enterprise, NGN is required to forward geographical location information received from an NGCN and possibly use it for routing to appropriate authorities. This can be subject to both privacy and regulatory requirements.

3) Routing of communications identified as emergency telecommunications in private network traffic is outside the scope of NGN documents. NGN is required not to handle such communication. This also applies to a hosted NGCN capability.

4) According to national regulations and laws, private numbering plans or dialling plans used within an enterprise can optionally reuse national emergency numbers for other purposes and can optionally use a different number to denote an emergency telecommunication.

5) According to national regulations and laws, where an enterprise operates a private PSAP, NGN can optionally support routing of public network traffic emergency telecommunication for enterprise to the private PSAP (or to one of several private PSAPs) or to a public PSAP, depending on circumstances. For example, for a caller physically located within a particular enterprise site, routing to the private PSAP for that site may be required, whereas for callers physically located elsewhere, routing to a public PSAP may be required.

20.5 User identifier presentation and privacy

1) NGN is required to have the capability to present the identifier of the originating party.

2) NGN is required to have the capability to present the identifier of the terminating party.

3) NGN is required to have the capability to suppress the presentation of the identifier of the originating party.

4) NGN is required to have the capability to suppress the presentation of the identifier of the terminating party.

NOTE – The requirements for support of emergency telecommunication may override the suppression.

20.6 Network or service provider selection

NGN is required to support the capability for provider selection, where required (e.g., by regulation or law).

20.7 Users with disabilities

Users with disabilities have a general need to be provided with means to control and use terminals and services in alternative ways and modes, suiting varied capabilities and preferences. Such requirements are best met by inclusive design of the general provision of terminals and services.

1) NGN is required to provide the means needed for invocation of relay services. Relay services translate between various modes of telecommunication that are of interest for people with disabilities (e.g., sign language, lip reading, text, voice). Invocation of relay services may be based on user preferences, address resolution or user commands.

2) NGN is required to have the capability to invoke relay services by either party in an emergency telecommunication.

NOTE 1 – Other needs for users with disabilities to use emergency telecommunication services are handled in clause 20.4.

NOTE 2 – See also [b-ITU-T Accessibility] and [b-ITU-T F.790].

20.8 Number portability

Number portability is a PSTN/ISDN network capability.

The equivalent capability in NGN is identifier portability (clause 10.2). PSTN/ISDN emulation places no new requirements to support number portability because emulated services are inherited from the PSTN/ISDN (see clause 19.1.3).

20.9 Service unbundling

In many national jurisdictions, it is required that service providers "unbundle" their offerings to allow customers a choice of providers for diverse services, as well as allow providers to competitively offer their services to customers.

Where required, e.g., by regulation or law, NGN is required to support mechanisms to realize service unbundling.

20.10 Anonymous communication rejection

NGN is required to provide a mechanism to allow a user to reject incoming communication when the caller is anonymous.

20.10.1 Anonymous communication rejection for enterprise

A communication identified as public network traffic is required to be handled in accordance with the anonymous communication rejection requirements of NGN.

Requirements for handling of anonymous communication in private network traffic are outside the scope of this Recommendation. NGN is required not to handle such communication. This also applies to a hosted NGCN capability.

NOTE – Separate regulatory requirements can optionally apply for private network traffic.

Appendix I

Main differences in terms of high-level requirements and capabilities between this version of Recommendation ITU-T Y.2202 (Y.2201 Rev.1) and the previous version of Recommendation ITU-T Y.2201 (2007)

(This appendix does not form an integral part of this Recommendation)

This appendix lists the main differences in terms of high-level requirements and capabilities between this Recommendation and ITU-T Y.2201 (04/07) [ITU-T Y.2201].

NOTE – Completion of this appendix is for further study.

ITU-T Y.2201 Rev.1 Capability	Clause in this Recommendation	Clause in ITU-T Y.2201 (2007) (if applicable)	Enhancements from Y.2201 (2007)	New capability
OAM			None	–
Mobility			Handover support	–
Context awareness		–	–	X

Appendix II

Mapping of services to service enablers

(This appendix does not form an integral part of this Recommendation)

NOTE – Completion of this appendix is for further study.

This appendix provides an example mapping of selected services to selected service enablers (clause 7.2). The mapping is not meant to be exhaustive nor represent requirements for support.

Table II.1 – Illustrative mapping of services to service enablers

Services/service enablers	Presence	Location management	Group management	Message handling	Multicast support	Push	Session handling	Personal information management	Device management	Web-based application support	Data synchronization
Real-time conversational voice services							X				
Real-time multimedia conversational services							X				
Real-time text							X				
Messaging services	X		X	X			X				
Push-to-talk over NGN	X		X				X				
Point-to-point interactive multimedia services			X				X				
Collaborative interactive communication services		X	X				X				
Push-based services		X				X					

Table II.1 – Illustrative mapping of services to service enablers

Services/service enablers	Presence	Location management	Group management	Message handling	Multicast support	Push	Session handling	Personal information management	Device management	Web-based application support	Data synchronization
Broadcast/multicast services					X						
Information services	X	X				X					
Presence and general notification services	X	X	X								
3GPP release 6 and 3GPP2 release A OSA-based services	X	X	X	X	X	X	X				
Data retrieval applications	X					X					
VPN services			X		X						
Applications and services using tag-based identification					X				X		
Visual surveillance services							X		X		
IPTV services											
Enterprise services: Virtual leased line service											
Enterprise services: Business trunking application											
Enterprise services: Hosted services for enterprises											
Managed delivery services											

Bibliography

The following documents contain information that may be valuable to the reader of this Recommendation. They provide additional information about topics covered within this Recommendation, but are not essential for an understanding of this Recommendation.

ITU Recommendations

[b-ITU-T E.351] Recommendation ITU-T E.351 (2000), *Routing of multimedia connections across TDM-, ATM- and IP-based networks*.

[b-ITU-T F.703] Recommendation ITU-T F.703 (2000), *Multimedia conversational services*.

[b-ITU-T F.724] Recommendation ITU-T F.724 (2005), *Service description and requirements for videotelephony services over IP networks*.

[b-ITU-T F.733] Recommendation ITU-T F.733 (2005), *Service description and requirements for multimedia conference services over IP networks*.

[b-ITU-T F.741] Recommendation ITU-T F.741 (2005), *Service description and requirements for audiovisual on-demand services*.

[b-ITU-T F.742] Recommendation ITU-T F.742 (2005), *Service description and requirements for distance learning services*.

[b-ITU-T F.790] Recommendation ITU-T F.790 (2007), *Telecommunications accessibility guidelines for older persons and persons with disabilities*.

[b-ITU-T Climate] ITU-T ICTs and Climate Change (2009), *Deliverable 2: Gap Analysis and Standards Roadmap*.

[b-ITU-T G.729A] Recommendation ITU-T G.729 Annex A (1996), *Reduced complexity 8 kbit/s CS-ACELP speech codec*.

[b-ITU-T G.780] Recommendation ITU-T G.780/Y.1351 (2004), *Terms and definitions for synchronous digital hierarchy (SDH) networks*.

[b-ITU-T G.799.1] Recommendation ITU-T G.799.1/Y.1451.1 (2004), *Functionality and interface specifications for GSTN transport network equipment for interconnecting GSTN and IP networks*.

[b-ITU-T G.805] Recommendation ITU-T G.805 (2000), *Generic functional architecture of transport networks*.

[b-ITU-T G.809] Recommendation ITU-T G.809 (2003), *Functional architecture of connectionless layer networks*.

[b-ITU-T G.1000] Recommendation ITU-T G.1000 (2001), *Communications Quality of Service: A framework and definitions*.

[b-ITU-T G.1010] Recommendation ITU-T G.1010 (2001), *End-user multimedia QoS categories*.

[b-ITU-T H.510] Recommendation ITU-T H.510 (2002), *Mobility for H.323 multimedia systems and services*.

[b-ITU-T H-Sup.1] ITU-T H-series Recommendations – Supplement 1 (1999), *Application profile – Sign language and lip-reading real-time conversation using low bit rate video communication*.

[b-ITU-T I.230] Recommendation ITU-T I.230 (1988), *Definition of bearer service categories*.

[b-ITU-T I.250] Recommendation ITU-T I.250 (1988), *Definition of supplementary services*.

[b-ITU-T I.570] Recommendation ITU-T I.570 (1993), *Public/private ISDN interworking*.

[b-ITU-T M.3017] Recommendation ITU-T M.3017 (2003), *Framework for the integrated management of hybrid circuit/packet networks*.

[b-ITU-T Q.833.1] Recommendation ITU-T Q.833.1 (2001), *Asymmetric digital subscriber line (ADSL) – Network element management: CMIP model*.

[b-ITU-T Q.1200] Recommendation ITU-T Q.1200 Series (1997), *General series Intelligent Network Recommendation structure*.

[b-ITU-T Q.1236] Recommendation ITU-T Q.1236 (1999), *Intelligent Network Capability Set 3 – Management Information Model Requirements and Methodology*.

[b-ITU-T Q.1702] Recommendation ITU-T Q.1702 (2002), *Long-term vision of network aspects for systems beyond IMT-2000*.

[b-ITU-T Q.1741.1] Recommendation ITU-T Q.1741.1 (2002), *IMT-2000 references to release 1999 of GSM evolved UMTS core network with UTRAN access network*.

[b-ITU-T Q.1741.2] Recommendation ITU-T Q.1741.2 (2002), *IMT-2000 references to release 4 of GSM evolved UMTS core network with UTRAN access network*.

[b-ITU-T Q.1741.3] Recommendation ITU-T Q.1741.3 (2003), *IMT-2000 references to release 5 of GSM evolved UMTS core network*.

[b-ITU-T Q.1741.4] Recommendation ITU-T Q.1741.4 (2005), *IMT-2000 references to release 6 of GSM evolved UMTS core network*.

[b-ITU-T Q.1742.4] Recommendation ITU-T Q.1742.4 (2005), *IMT-2000 references (approved as of 30 June 2004) to ANSI-41 evolved core network with cdma2000 access network*.

[b-ITU-T Q.1761] Recommendation ITU-T Q.1761 (2004), *Principles and requirements for convergence of fixed and existing IMT-2000 systems*.

[b-ITU-T T.140] Recommendation ITU-T T.140 (1998), *Protocol for multimedia application text conversation*.

[b-ITU-T X.501] Recommendation ITU-T X.501 (2008) | ISO/IEC 9594-2:2008, *Information technology – Open Systems Interconnection – The Directory: Models*.

[b-ITU-T X.509] Recommendation ITU-T X.509 (2008) | ISO/IEC 9594-8:2008, *Information technology – Open Systems Interconnection – The Directory: Public-key and attribute certificate frameworks*.

[b-ITU-T X.511] Recommendation ITU-T X.511 (2008) | ISO/IEC 9594-3:2008, *Information technology – Open Systems Interconnection – The Directory: Abstract service definition*.

[b-ITU-T X.1244] Recommendation ITU-T X.1244 (2008), *Overall aspects of countering spam in IP-based multimedia applications*.

[b-ITU-T Y.1411] Recommendation ITU-T Y.1411 (2003), *ATM-MPLS network interworking – Cell mode user plane interworking*.

[b-ITU-T Y.2052] Recommendation ITU-T Y.2052 (2008), *Framework of multi-homing in IPv6-based NGN*.

[b-ITU-T Y.2053] Recommendation ITU-T Y.2053 (2008), *Functional requirements for IPv6 migration in NGN*.

[b-ITU-T Y.2054] Recommendation ITU-T Y.2054 (2008), *Framework to support signalling for IPv6-based NGN*.

[b-ITU-T Y-Sup.1] ITU-T Y.2000-series Recommendations – Supplement 1 (2006), *ITU-T Y.2000 series – Supplement on NGN release 1 scope*.

[b-ITU-T Y-Sup.5] ITU-T Y.1900 series Recommendations – Supplement 5 (2008), *ITU-T Y.1900-series – Supplement on IPTV service use cases*.

[b-ITU-T Y-Sup.7] ITU-T Y-series Recommendations – Supplement 7 (2008), *ITU-T Y.2000 series – Supplement on NGN release 2 scope*.

[b-ITU-R M.1645] Recommendation ITU-R M.1645 (2003), *Framework and overall objectives of the future development of IMT-2000 and systems beyond IMT-2000*.

ITU-T guidelines

[b-ITU-T Accessibility] ITU-T Technical Paper (2006), *FSTP-TACL Telecommunications Accessibility Checklist*.

ETSI technical specifications

[b-ETSI TR 121 905] ETSI TR 121 905 V7.3.0 (2007), *Digital cellular telecommunications system (Phase 2+); Universal Mobile Telecommunications System (UMTS); Vocabulary for 3GPP Specifications*.

[b-ETSI TS 101 331] ETSI TS 101 331 V1.2.1 (2006), *Lawful Interception (LI); Requirements of Law Enforcement Agencies*.

[b-ETSI TS 122 057] ETSI TS 122 057 V6.0.0 (2005), *Digital cellular telecommunications system (Phase 2+); Universal Mobile Telecommunications System (UMTS); Mobile Execution Environment (MExE) service description; Stage 1*.

[b-ETSI TS 122 071] ETSI TS 122 071 V3.5.0 (2004), *Digital cellular telecommunications system (Phase 2+); Universal Mobile Telecommunications System (UMTS); Location Services (LCS); Stage 1*.

[b-ETSI TS 122 078] ETSI TS 122 078 V7.6.0 (2005), *Digital cellular telecommunications system (Phase 2+); Universal Mobile Telecommunications System (UMTS); Customized Applications for Mobile network Enhanced Logic (CAMEL); Service description*.

[b-ETSI TS 122 127] ETSI TS 122 127 V7.1.0 (2006), *Universal Mobile Telecommunications System (UMTS); Service requirement for the Open Services Access (OSA); Stage 1*.

[b-ETSI TS 122 140] ETSI TS 122 140 V6.7.0 (2005), *Universal Mobile Telecommunications System (UMTS); Multimedia Messaging Service (MMS); Stage 1*.

[b-ETSI TS 122 146] ETSI TS 122 146 V7.2.0 (2006), *Digital cellular telecommunications system (Phase 2+); Universal Mobile Telecommunications System (UMTS); LTE; Multimedia Broadcast/Multicast Service (MBMS); Stage 1*.

[b-ETSI TS 122 174] ETSI TS 122 174 V6.2.0 (2005), *Digital cellular telecommunications system (Phase 2+); Universal Mobile Telecommunications System (UMTS); Push service; Stage 1*.

[b-ETSI TS 122 240] ETSI TS 122 240 V6.5.0 (2005), *Universal Mobile Telecommunications System (UMTS); Service requirements for 3GPP Generic User Profile (GUP); Stage 1*.

[b-ETSI TS 122 250] ETSI TS 122 250 V6.0.0 (2005), *Universal Mobile Telecommunications System (UMTS); IP Multimedia Subsystem (IMS) Group Management; Stage 1*.

[b-ETSI TS 123 141] ETSI TS 123 141 V7.2.0 (2006), *Universal Mobile Telecommunications System (UMTS); Presence service; Architecture and functional description; Stage 2*.

[b-ETSI TS 123 228] ETSI TS 123 228 V7.7.0 (2007), *Digital cellular telecommunications system (Phase 2+); Universal Mobile Telecommunications System (UMTS); IP Multimedia Subsystem (IMS); Stage 2*.

[b-ETSI TS 126 235] ETSI TS 126 235 V6.4.0 (2005), *Digital cellular telecommunications system (Phase 2+); Universal Mobile Telecommunications System (UMTS); Packet switched conversational multimedia applications; Default codecs*.

[b-ETSI TS 133 106] ETSI TS 133 106 V7.0.1 (2006), *Universal Mobile Telecommunications System (UMTS); Lawful interception requirements*.

[b-ETSI TS 142 033] ETSI TS 142 033 V7.0.0 (2007), *Digital cellular telecommunications system (Phase 2+); Lawful Interception; Stage 1*.

[b-ETSI TS 181 005] ETSI TS 181 005 V2.4.1 (2007), *Telecommunications and Internet Converged Services and Protocols for Advanced Networking (TISPAN); Service and Capability Requirements*.

[b-ETSI TS 181 019] ETSI TS 181 019 V2.0.0 (2007), *Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); Business Communication Requirements*.

[b-ETSI TS 187 009] ETSI TS 187 009 V2.1.1 (2008), *Telecommunications and Internet Converged Services and Protocols for Advanced Networking (TISPAN); Feasibility study of prevention of unsolicited communication in the NGN*.

American National Standards Institute (ANSI) standards

[b-ANSI-J-STD-025] ANSI-J-STD-025-A-2003, *Lawfully Authorized Electronic Surveillance (CALEA)*.

[b-ATIS 1000678] ATIS 1000678-2006, *Lawfully Authorized Electronic Surveillance (LAES) for Voice over Packet Technologies in Wireline Telecommunications Networks, Version 2*.

[b-T1.724] ANSI T1.724-2004, *UMTS Handover Interface for Lawful Interception*.

[b-TIA-127-A] TIA-127-A (2004), *Enhanced Variable Rate Codec Speech Option 3 for Wideband Spread Spectrum Digital Systems*.

[b-TIA-1016-A] TIA-1016-A (2006), *Source-Controlled Variable-Rate Multimode Wideband Speech Codec (VMR-WB) – Service Options 62 and 63 for Spread Spectrum Systems*.

[b-TIA-1066] TIA-1066 (2006), *LAES for cdma2000 VoIP*.

[b-TIA-1072] TIA-1072 (2006), *LAES for cdma2000 push-to-talk over cellular*.

IETF specifications

[b-IETF RFC 2486] IETF RFC 2486 (1999), *The Network Access Identifier*.

[b-IETF RFC 4594] IETF RFC 4594 (2006), *Configuration Guidelines for DiffServ Service Classes*.

Open Mobile Alliance specifications

[b-OMA-DS] OMA specification (2006), *Data Synchronization V1.2*.

[b-OMA-DM] OMA specification (2007), *Device Management V1.2*.

[b-OMA-OSE] OMA specification (2007), *Service Environment V1.0*.

[b-OMA-PoC] OMA specification (2006), *Push to talk over Cellular V1.0.1*.

[b-OMA-PS] OMA specification (2006), *Presence Simple V1.0.1*.

[b-OMA-WS] OMA specification (2006), *Web Services V1.1*.

[b-OMA-XML] OMA specification (2006), *XML Document Management*.

[b-OMA-LS] OMA specification (2006), *Mobile Location Service V1.1*.

[b-OMA-XDM] OMA specification (2006), *XML Document Management V1.0.1*.

[b-OMA-Push] OMA specification (2005), *Push V2.1*.

Open Service Access (OSA)

[b-OSA-Parlay-X] ETSI ES 202 391-x (2006), *Open Service Access (OSA), Parlay X Web Services, Parts 1-14*.

[b-OSA-Parlay-4] ETSI ES 202 915-x V1.3.1 (2006), *Open Service Access (OSA); Application Programming Interface (API); Parts 1-14 (Parlay 4)*.

[b-OSA-Parlay-5] ETSI ES 203 915-x V1.1.1 (2007), *Open Service Access (OSA); Application Programming Interface (API); Parts 1-15 (Parlay 5)*.

IN services

[b-TIA/EIA/IS-771-1] TIA/EIA/IS 771-1 (1999), *Wireless Intelligent Network – Addendum 1 (2001)*.

[b-TIA-873.002] TIA-873.002 (2003), *All IP Core Network Multimedia Domain – IP Multimedia Subsystem – Stage-2 (2003)*.

UDDI specifications

[b-OASIS-UDDI] OASIS specification (2004), *UDDI Version 3.0.2*.

SOA specifications

[b-OASIS-SOA] OASIS specification (2006), *Reference Model for Service Oriented Architecture 1.0*.

SERIES OF ITU-T RECOMMENDATIONS

Series A	Organization of the work of ITU-T
Series D	General tariff principles
Series E	Overall network operation, telephone service, service operation and human factors
Series F	Non-telephone telecommunication services
Series G	Transmission systems and media, digital systems and networks
Series H	Audiovisual and multimedia systems
Series I	Integrated services digital network
Series J	Cable networks and transmission of television, sound programme and other multimedia signals
Series K	Protection against interference
Series L	Construction, installation and protection of cables and other elements of outside plant
Series M	Telecommunication management, including TMN and network maintenance
Series N	Maintenance: international sound programme and television transmission circuits
Series O	Specifications of measuring equipment
Series P	Terminals and subjective and objective assessment methods
Series Q	Switching and signalling
Series R	Telegraph transmission
Series S	Telegraph services terminal equipment
Series T	Terminals for telematic services
Series U	Telegraph switching
Series V	Data communication over the telephone network
Series X	Data networks, open system communications and security
Series Y	**Global information infrastructure, Internet protocol aspects and next-generation networks**
Series Z	Languages and general software aspects for telecommunication systems

Printed in Switzerland
Geneva, 2010