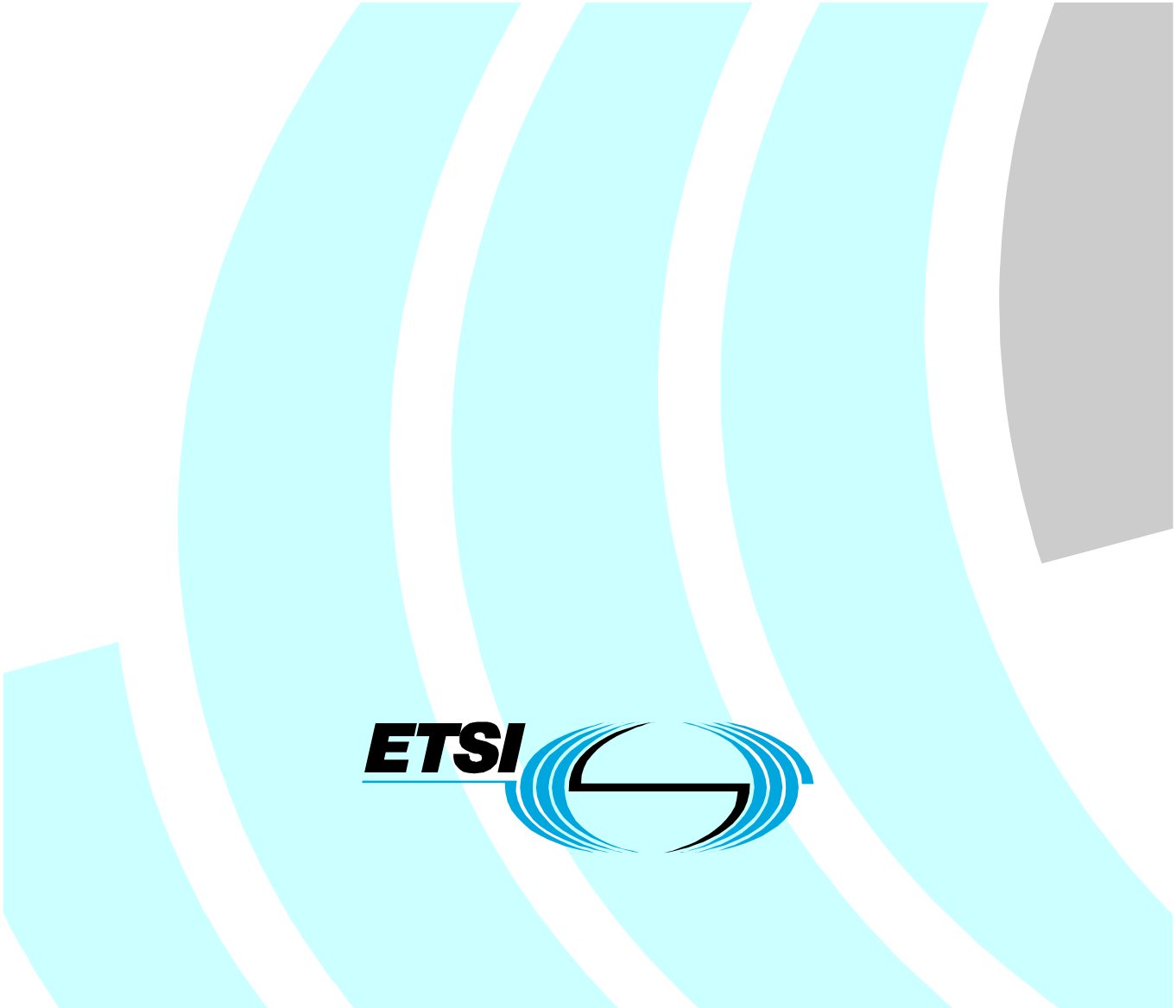
ETSI TS 188 003 V1.1.1 (2005-09)

Technical Specification

Telecommunications and Internet Converged Services and Protocols for Advanced Networking (TISPAN); OSS requirements; OSS definition of requirements and priorities for further network management specifications for NGNOSS definition of requirements and priorities for further network management specifications for NGN



Reference
DTS/TISPAN-08004-NGN

Keywords
management, network, remote

ETSI

650 Route des Lucioles
F-06921 Sophia Antipolis Cedex - FRANCE

Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16

Siret N° 348 623 562 00017 - NAF 742 C
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° 7803/88

Important notice

Individual copies of the present document can be downloaded from:
http://www.etsi.org

The present document may be made available in more than one electronic version or in print. In any case of existing or perceived difference in contents between such versions, the reference version is the Portable Document Format (PDF). In case of dispute, the reference shall be the printing on ETSI printers of the PDF version kept on a specific network drive within ETSI Secretariat.

Users of the present document should be aware that the document may be subject to revision or change of status. Information on the current status of this and other ETSI documents is available at
http://portal.etsi.org/tb/status/status.asp

If you find errors in the present document, please send your comment to one of the following services:
http://portal.etsi.org/chaircor/ETSI_support.asp

Copyright Notification

Contents

Intellectual Property Rights

IPRs essential or potentially essential to the present document may have been declared to ETSI. The information pertaining to these essential IPRs, if any, is publicly available for **ETSI members and non-members**, and can be found in ETSI SR 000 314: *"Intellectual Property Rights (IPRs); Essential, or potentially Essential, IPRs notified to ETSI in respect of ETSI standards"*, which is available from the ETSI Secretariat. Latest updates are available on the ETSI Web server (http://webapp.etsi.org/IPR/home.asp).

Pursuant to the ETSI IPR Policy, no investigation, including IPR searches, has been carried out by ETSI. No guarantee can be given as to the existence of other IPRs not referenced in ETSI SR 000 314 (or the updates on the ETSI Web server) which are, or may be, or may become, essential to the present document.

Foreword

This Technical Specification (TS) has been produced by ETSI Technical Committee Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN).

1 Scope

The present document identifies NGN OSS requirements and consolidates and categorizes them.

Annex B contains an unstructured list of requirements as identified and extracted from numerous sources.

Annex A contains a list of consolidated requirements. These requirements represent a first analysis of the requirements captured in annex B where duplications and overlaps have been removed and complex requirements split into single purpose requirements. Annex A is used as the basis of the requirements categorization in clause 4.

Clause 4 structures the requirements into a hierarchy (level 0, 1 or 2 requirements) and categorizes them on how they fulfil the NGN Management Vision. It should be noted that individual requirements may be mapped to more than 1 category, where the requirements impacts several areas.

In annex A and clause 4 those requirements that impact the development TISPAN_NGN release 1 are identified.

2 References

The following documents contain provisions which, through reference in this text, constitute provisions of the present document.

- References are either specific (identified by date of publication and/or edition number or version number) or non-specific.
- For a specific reference, subsequent revisions do not apply.
- For a non-specific reference, the latest version applies.

Referenced documents which are not found to be publicly available in the expected location might be found at http://docbox.etsi.org/Reference.

[1] ETSI TR 188 004: "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); NGN Management; OSS vision".

[2] ETSI TR 180 001: "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); NGN Release 1; Release definition".

[3] ITU-T Recommendation M.3050: "Enhanced Telecommunications Operations Map".

[4] ETSI TS 132 101: "UMTS; Telecommunication management; Principles and high level requirements".

[5] ETSI TS 132 102: "UMTS; Telecommunication management; Architecture".

[6] ETSI TS 101 303: "Telecommunications and Internet Protocol Harmonization Over Networks (TIPHON) Release 4; Service Independent Requirements Definition; Service and Network Management Framework; Overview and Introduction".

3 Definitions and abbreviations

3.1 Definitions

For the purposes of the present document, the following terms and definitions apply:

access network: collection of network entities and interfaces that provides the underlying IP transport connectivity between the device and the NGN entities

NOTE: An example of an "Access Network" is ADSL.

core network: portion of the delivery system composed of networks, systems equipment and infrastructures, connecting the service providers to the access network

NOTE: The core network is independent of the connection technology of the terminal (e.g. radio, WLAN, xDSL, etc.)

administrative domain: collection of physical or functional entities under the control of a single administration

customer: role that contracts for the services offered by a service provider based on a contractual relationship

mobility: ability for the user to communicate and access the same services irrespective of changes of the location or access technology capabilities with or without service continuity

nomadism: ability of the user to change his 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 session continuity or hand-over possible

NOTE: It is assumed that normal usage pattern is that users shutdown their service session before moving to another access point.

roaming: ability of users to access services while outside of their subscribed home network, i.e. by using an access point of a visited network

NOTE: This is usually supported by a roaming agreement between the respective network operators.

service provider: entity that offers services to users involving the use of network resources

User Equipment (UE): device allowing a user access to network services

3.2 Abbreviations

For the purposes of the present document, the following abbreviations apply:

ALC	Automatic Level Control
CCV	Common Communications Vehicle
CMIP	Common Management Information Protocol
CORBA	Common Object Request Broker Architecture
DSL	Digital Subscriber Line
ebXML	e-business XML
ENUM	Electronic Number (RFC 2916)
IAD	Integrated Access Devices
IETF	Internet Engineering Task Force
ITU-T	International Telecommunication Union - Telecommunication sector
MCU	Media Control Unit
MEGACO	MEdia GAteway COntrol protocol
MGCP	Media Gateway Control Protocol
MPLS	Multi Protocol Label Switching
NGN	Next Generation Networks
NGOSS	New Generation Operations Systems and Software
OLO	Other Licensed Operator
OSS	Operations Support System
PSTN	Public Switched Telephone Networks
QoS	Quality of Service
SIP	Session Initiated Protocol
SNMP	Simple Network Management Protocol
UE	User Equipment
UMTS	Universal Mobil Telecommunications System
WLAN	Wireless Local Area Network
XML	eXtended Mark up Language

4 Structured requirements

In this clause the unstructured requirements contained in annex A are structured as follows:

- At the highest level, the requirements are grouped into Business Vision requirements, Customer Centric requirements, Technology requirements, Operational requirements and Regulatory requirements (level 0).
- The more general requirements, in the unstructured list, are mapped to the "High level Requirements (level 1)".
- The more detailed requirements are listed as "level 2" requirements supporting these "level 1" requirements.

The level 0 and level 1 requirements are structured as follows:

Level 0 Requirements	o **Level 1 Requirements**
To support the Business Vision requirements	o Support Value Chains of Multiple Service Providers: Multiple Trading Partners with Complex Value Chains and Business Models o Support for a wide range of services, applications and mechanisms o Support of real time/streaming/non-real time and multimedia services o Enrich product offering with contextual information, e.g. location and presence o Shortened product lifecycle
To support the Customer Centric requirements	o Access to services at any time, any place, through any chosen access mechanism and terminal (user equipment) o Personalization of services based on access mechanism and terminal (user equipment) o Security of personal information o Unified service characteristics for the same service as perceived by the user o Self Service capabilities allowing to aggregate services form different providers o Simple and straightforward conceptual model of services to be created and presented to customers o Straightforward billing models that are easily related to events and configuration changes that the customer can understand, or has access to, and that form part of the simple service description o Customer data might be spread across multiple networks across the value chain o Single Sign On o Mobility
To support the Technology requirements	o Multi-media services over packet-based transfer o Independence of service-related functions from underlying transport o Separation of control functions o Broadband capabilities o Interworking with legacy networks via open interfaces o Support of multiple last mile technologies o Convergence of fixed and mobile, TDM and packet-based services o Support a variety of identification schemes o Terminal (user equipment) Management
To support the Operational requirements	o End-to-end QoS o Subscriber Data Management with consolidation of information across the infrastructure and federation of data across the value chain o Problems to be reported in the context of the simple and straightforward service models o Perfect touch and zero fall-out o Automated Service Creation processes o Management of NGN resources (physical and logical)
Regulatory requirements	o Emergency communications o Security o Privacy o Lawful interception o Unrestricted access by users to different service providers

4.1 Customer Centric requirements

Req	Requirement	Release 1	Comments
A15	Management systems shall be capable of supporting customer segmentation in the 10 000's.		
A25	Products codes shall not be tied 1 to 1 with specific tariffs.	Y	

4.1.1 Access to services at any time, any place, through any chosen access mechanism and terminal (user equipment)

Req	Requirement	Release 1	Comments
A21	Management processes shall support the User Access control and trust Processes.	Y	
A23	Management processes shall support "off-net" presentation by users.		
A37	management shall provide a processes to support a customer wishing to check their subscription configuration.		
A72	Customer Hotline.		
A78	Supporting the availability of management services any place any time to any authorized organization or individual (e.g. access to billing records shall be available 24/7).	Y	

4.1.2 Personalization of services based on access mechanism and terminal (user equipment)

Req	Requirement	Release 1	Comments
A6	Management of Personalization of Services.	Y	
59	To be able to discover limitations imposed by the terminal (user equipment) that the user has connected. (Analogue phone, IP Phone, PC).	Y	
A60	Discovery of the configuration (physical and logical) of an access segment including the source of configuration data.	Y	To be able to discover which ingress node applies for a particular endpoint or access segment and where admission control is applied. And how it is configured for that endpoint or access segment. To be able to discover the information source used to configure the above and discover the data it contains. To be able to compare the two. To be able to discover the current loading of ingress/admission elements and of queues. Where appropriate, to be able to discover alternate/fallback entities and equipment?
A77	Providing the management capabilities which will enable organizations offering NGN end user services to offer customers the ability to personalize end user services and to create new services from service capabilities (potentially from different service providers).	Y	

4.1.3 Security of personal information

Req	Requirement	Release 1	Comments
A33	Management of the subscription related aspects of the user profile (subscription profile) including ownership of components.	Y	subscription profile components will be needed for: data related to subscription identification and numbering. E.g. private identity, public identity, registration status; data related to roaming; data related to authentication and ciphering; data related to SPOA selection information; data related to applications and service triggers.
A35	Subscription management shall be able to control the ownership of components common to the user profile and the subscription profile.	Y	
A36	Modifications by the subscription management to subscription profile components shall be recorded in an historical log.	Y	
A42	Access to customer information shall only be permitted in an authorized and secure manner.	Y	

4.1.4 Unified service characteristics for the same service as perceived by the user

Req	Requirement	Release 1	Comments
A84	Unified service characteristics for the same service as perceived by the user.	Y	

4.1.5 Self Service capabilities allowing to aggregate services form different providers

Req	Requirement	Release 1	Comments
A77	Providing the management capabilities which will enable organizations offering NGN end user services to offer customers the ability to personalize end user services and to create new services from service capabilities (potentially from different service providers).	Y	
A79	Supporting eBusiness Value Networks based upon concepts of business roles (Customer, Service Provider, Complementor, Intermediary, Supplier (e.g. Equipment Vendor)) (ITU-T Recommendations Y.110 (see Bibliography) and M.3050 [3]).	Y	

4.1.6 Simple and straightforward conceptual model of services to be created and presented to customers

Req	Requirement	Release 1	Comments
A16	Management of User Profile information shall allow distribution amongst networks, OSS, admin domains and end user terminals (user equipment).	Y	

4.1.7 Straightforward billing models that are easily related to events and configuration changes that the customer can understand, or has access to, and that form part of the simple service description

Req	Requirement	Release 1	Comments
A24	Support multiple billing models, including billing on behalf of others.	Y	
A69	Bill limitations It can be necessary to protect users from bills of unexpected amounts. Further it may be necessary to protect users from misuse of their accounts, and to protect operators from misuse of services.		
A83	Supporting the collection of charging data for the network operator regarding the utilization of resources in the network either for later use by billing processes (offline charging) or for near-real time interactions with rating applications (online charging).	Y	

4.1.8 Customer data might be spread across multiple networks across the value chain

Req	Requirement	Release 1	Comments
A16	Management of User Profile information shall allow distribution amongst networks, OSS, admin domains and end user terminals (user equipment).	Y	
A22	Management processes shall support dynamic association of access points with User Profile and Subscription information.	Y	

4.1.9 Single Sign On

Req	Requirement	Release 1	Comments
A89	Single sign on		

4.1.10 Mobility

Req	Requirement	Release 1	Comments
A5	Management of Mobility	Y (see note)	Only nomadism required for release 1 (i.e. no support for hand-over of communications sessions between access networks).
NOTE: There are significant impacts in the security and personalization aspects of the services.			

4.2 Business Vision Requirements

4.2.1 Support Value Chains of Multiple Service Providers: Multiple Trading Partners with Complex Value Chains and Business Models

Req	Requirement	Release 1	Comments
A10	Management of storage distribution of applications and content using Digital Rights.		These shall cover access control, user and content owners policy and support for creating accounting records for user by users and content application providers of users and management
A24	Support multiple billing models, including billing on behalf of others.	Y	
A26	Value Chain technology Support for varying and changing business models shall be supported.	Y	
A27	For B2B, the use of main stream e-commerce solutions shall be supported.	Y	
A34	control the capabilities that need to be offered to Business to Business (B2B) trading partners, such as value add service providers.		

Req	Requirement	Release 1	Comments
A39	Interfaces between trading partners shall meet the commercial and legal standards required for the business to business transactions.	Y	Focus on Accounting and Billing for R1
A40	Interfaces supporting relationships between organizations shall use mainstream e-commerce technology methods.	Y	
A79	Supporting eBusiness Value Networks based upon concepts of business roles (Customer, Service Provider, Complementor, Intermediary, Supplier (e.g. Equipment Vendor)) (ITU-T Recommendations Y.110 and M.3050 [3]).	Y	
A80	Allowing an enterprise and/or an individual to adopt multiple roles in different value networks and also multiple roles within a specific value network (e.g. one role as a retail Service Provider and another role as a wholesale Service Provider) (ITU-T Recommendation M.3050 [3]).	Y	

4.2.2 Support for a wide range of services, applications and mechanisms

Req	Requirement	Release 1	Comments
A9	Supporting the management Parlay v 4.0 APIs.		
A18	Service Detail Records and Product codes need to be managed in the 1 000's.		

4.2.3 Support of real time/streaming/non-real time and multimedia services

Req	Requirement	Release 1	Comments
A11	Management of end to end VPN solutions.	Y	
A85	Support TISPAN Release 1 Services.	Y	

4.2.4 Enrich product offering with contextual information, e.g. location and presence

Req	Requirement	Release 1	Comments
A6	Management of Personalization of Services.	Y	
A7	Management of Location and context Services.	Y	

4.2.5 Shortened product lifecycle

Req	Requirement	Release 1	Comments
A20	Management processes shall support and automate Product Lifecycle Management.	Y	

4.3 Technology requirements

4.3.1 Multi-media services over packet-based transfer

Req	Requirement	Release 1	Comments
A2	Management of end to end connectivity (Transport).	Y	

4.3.2 Independence of service-related functions from underlying transport

Req	Requirement	Release 1	Comments
A8	Management of NGN Service Layer entities.	Y	
A82	Integrating an abstracted view on Resources (network, computing and application), which is hiding complexity and multiplicity of technologies and domains in the resource layer.	Y	

4.3.3 Separation of control functions

Req	Requirement	Release 1	Comments
A4	Management of Session Control, Media Control and Bearer Control.	Y	

4.3.4 Broadband capabilities

Req	Requirement	Release 1	Comments
A85	Support TISPAN Release 1 Services.	Y	

4.3.5 Interworking with legacy networks via open interfaces

Req	Requirement	Release 1	Comments
A81	Allowing the management of hybrid networks comprising NGN and non-NGN (e.g. PSTN, cable network) resources.	Y	

4.3.6 Support of multiple last mile technologies

Req	Requirement	Release 1	Comments
A3	Support of multiple access technologies (including, as a minimum, Integrated access devices (IAD), DSL and WLAN access, gigabit Ethernet metro core networks).	Y	

4.3.7 Convergence of fixed and mobile, TDM and packet-based services

Req	Requirement	Release 1	Comments
A2	Management of end to end connectivity (Transport).	Y	

4.3.8 Support a variety of identification schemes

Req	Requirement	Release 1	Comments
A64	From the unique identifier (E164, ENUM etc.), to be able to trace, where applicable, current: log on name and password; network endpoint IP address and hardware address; terminal (user equipment) IP address and hardware address. And the reverse.		To be able to identify the functional entities (e.g. DNS, DHCP, and LDAP Server) responsible for: network log on; issue of IP address; configuration of terminal/soft client e.g. from user profile, for network capability; resolution of called party unique identifier e.g. E164, ENUM to transport address(es). And the physical equipment they are hosted on. To be able to discover current configuration data from those entities. Where appropriate, to be able to discover alternate/fallback equipments and entities. **Where a "chain of responsibility" exists, to be able to discover the next in line.**
A88	Support a variety of identification schemes.	FFS	

4.3.9 Terminal (user equipment) Management

Req	Requirement	Release 1	Comments
A1	Management of User Equipment (including configuration and downloading of applications and QoS).	Y	

4.4 Operational requirements

4.4.1 End-to-end QoS

Req	Requirement	Release 1	Comments
A12	Management of IP QoS across technical sub-domains and between operators.	Y	Interfaces between operators shall not assume a single end to end technical solution for IP QoS.
A13	Support the use of protection mechanisms in the Access, core, metro, backhaul and with OLOs.		

4.4.2 Subscriber Data Management with consolidation of information across the infrastructure and federation of data across the value chain

Req	Requirement	Release 1	Comments
A38	It shall be possible to replicate and distribute the subscription profile components following rules established and defined by subscription management feature.	Y	

4.4.3 Problems to be reported in the context of the simple and straightforward service models

Req	Requirement	Release 1	Comments
A31	Providing the management capabilities which will enable organizations offering NGN end user service improvements including customer self service (e.g. provision of service, reporting faults, online billing reports), SLA Enforcement.	Y	

4.4.4 Perfect touch and zero fall-out

Req	Requirement	Release 1	Comments
A88	Perfect touch and zero fall-out.		

4.4.5 Automated Service Creation processes

Req	Requirement	Release 1	Comments
A19	Management processes shall support flexible, transport technology agnostic, service creation environments.	Y	
A20	Management processes shall support and automate Product Lifecycle Management.	Y	
A28	The service creation process shall support the creation of (software) components whose services are exposed via contracts.	Y	
A29	The components created by the service creation process shall use a common information model.	Y	
A30	The service creation process shall support a directory (or trading) feature for contracts in order to facilitate the design of software from existing (Off the Shelf) components.	Y	
A31	Providing the management capabilities which will enable organizations offering NGN end user service improvements including customer self service (e.g. provision of service, reporting faults, online billing reports), SLA Enforcement.	Y	
A32	Enable reusability by definition of building blocks, which describe and represent unitary service features or network features.	Y	

4.4.6 Management of NGN resources (physical and logical)

Req	Requirement	Release 1	Comments
A41	To claim to be NGN compliant management interfaces shall be open and use industry standard solutions.	Y	
A55	To be able to discover the current policy decision and policy enforcement points for a given access segment/given customer.	Y	
A56	To be able to validate the current policy enforced within the network domain.	Y	
57	To be able to discover the policy being enforced in an adjacent service or customer domain.		
58	To be able to validate that the policies being enforced in an adjacent service or customer domain are compatible.		

Req	Requirement	Release 1	Comments
59	To be able to discover limitations imposed by the terminal (user equipment) that the user has connected. (Analogue phone, IP Phone, PC).	Y	
A60	Discovery of the configuration (physical and logical) of an access segment including the source of configuration data.	Y	To be able to discover which ingress node applies for a particular endpoint or access segment and where admission control is applied. And how it is configured for that endpoint or access segment. To be able to discover the information source used to configure the above and discover the data it contains. To be able to compare the two. To be able to discover the current loading of ingress/admission elements and of queues. Where appropriate, to be able to discover alternate/fallback entities and equipment.
A61	Discovery of the configuration (physical and logical) of the signalling routing.	Y	To be able to discover the two way routing of signalling between an endpoint and its call control entity, and identify any intermediate Gateways and Interworking Functions, including which network nodes they are hosted on. To be able to discover the current configuration of "Virtual circuits" e.g. MPLS. To be able to discover the current transport network route topology. To be able to use this information to infer the routing of media streams (both directions) for given endpoints, customers, service types.
A62	To be able to discover which egress node applies for specific called and calling party pairs.	Y	Note that where alternate routings apply there can be more than one possible egress node. To be able to discover the type and configuration of these egress nodes, especially any policy enforcement rules and related measurements. To be able to discover the current loading of egress elements and of their queues.
A63	Discovery of the configuration (physical and logical) of the core network.	Y	To be able to discover which instances of call controller; intermediate gateways/IWF; service quality management entities. currently apply for a particular endpoint or access segment, and which physical equipment they are currently hosted on. To be able to discover configuration data from them related to that endpoint or access segment. More work is needed to list out the key configuration information needed. However, it includes: records of improper call terminations and reason codes; call usage records; quality criteria currently applicable for endpoint, customer, service type. Both measurements and rules; in mobile IP, identification of past and present Foreign Agents and their transport addresses; see also addressing clause

Req	Requirement	Release 1	Comments
A64	From the unique identifier (E164, ENUM etc.), to be able to trace, where applicable, current: log on name and password; network endpoint IP address and hardware address; terminal (user equipment) IP address and hardware address. And the reverse.	Y	To be able to identify the functional entities (e.g. DNS, DHCP, and LDAP Server) responsible for: network log on; issue of IP address; configuration of terminal/soft client e.g. from user profile, for network capability; resolution of called party unique identifier e.g. E164, ENUM to transport address(es). And the physical equipment they are hosted on. To be able to discover current configuration data from those entities. Where appropriate, to be able to discover alternate/fallback equipments and entities. Where a "chain of responsibility" exists, to be able to discover the next in line.
A65	Fault management functions (including Alarm Surveillance) and associated managed objects shall be applicable to all NGN entities.	(see note)	Fault Management is outside the scope of NGN OSS Release 1.
A66	Under Crisis situations (either network related or external) the NGN shall continue to provide essential management information and accept management controls.	Y	
A67	NGN Management will exploit wherever possible the business and service processes as defined by the ITU-T and TeleManagement Forum (TMF) i.e. ITU-T Recommendation M.3050 [3].	Y	
A68	NGN Management will exploit wherever possible the management communication protocols and information bases already defined.	Y	
NOTE: Egress means here egress from the service provider/network operators Administrative Domain.			

4.5 Regulatory requirements

4.5.1 Emergency communications

Req	Requirement	Release 1	Categorized in paragraph	Comments
A14	Support national emergency services and international Emergency Telecommunications Services.		4.5.1	

4.5.2 Security

Req	Requirement	Release 1	Comments
A5	Management of Mobility.	Y (see note)	Only nomadism required for release 1 (i.e. no support for hand-over of communications sessions between access networks).
A21	Management processes shall support the User Access control and trust Processes.	Y	
A42	Access to customer information shall only be permitted in an authorized and secure manner.	Y	

Req	Requirement	Release 1	Comments
A43	Secure mechanisms shall be available for the transfer of data (e.g. customer data) to, from or between authorized entities and shall be appropriate to the level of confidentiality of the data, the endpoints of the transfer and the routes that are available for the transfer of the data. The owner of the data, normally the body storing the master copy of the data, shall be responsible for applying the appropriate level of security to the transfer of the data.	Y	
A44	Before any transfer takes place, it shall be possible for the sender of the data to verify the identity of the recipient.	Y	
A45	It shall be possible for the recipient of data to identify the sender.	Y	
A46	It is permissible for either the sender or recipient of data to employ the services of a third party, known to, and trusted by, both in order to provide authentication of identity.	Y	
A47	The validity of an authentication of identity shall, if required, be subject to a maximum time limit.	Y	
A48	It shall be possible for the sender of data to render the data to be unreadable by any party not authorized to receive it.	Y	
A49	It shall be possible for the recipient of data to detect whether the sender has made any change to the data subsequent to its transmission.	Y	
A50	The security mechanisms shall provide verification that the data has been sent by the sender and received by the recipient (non-repudiation).	Y	
A51	It shall be possible for the sender and/or the recipient to create an audit log of all data transfer transactions of a specified type, provided that this requirement is made known before any transfer takes place.	Y	
A52	Transaction security for the change of data should be available in order to ensure the consistent change of data at different locations.	Y	
A53	Management features will need to bridge between the NGN security functions and the security used in mainstream e-commerce solutions such as those in ebXML.		
A70	Secure billing administration.	Y	
A71	Authorization control (e.g. via black lists) to prevent fraud.	FFS	
A73	Support Security related reports to the user.		
A74	Contractual agreements relating to security issues can be included in the roaming agreement between two operators.		
A75	Contractual agreements between service providers and subscribers relating to security issues shall be included in the conditions for the subscription.	Y	
A76	A secure subscription process to restrict subscription fraud.	Y	
NOTE: There are significant impacts in the security and personalization aspects of the services.			

4.5.3 Privacy

Req	Requirement	Release 1	Comments
A17	Processes for distribution and synchronization of User Profile information shall enforce policies set by regulation, applicable data protection laws, users and operators.	Y	
A39	Interfaces between trading partners shall meet the commercial and legal standards required for the business to business transactions.	Y	Focus on Accounting and Billing for R1
A54	Management shall fulfil local privacy regulations.	Y	

4.5.4 Lawful interception

Req	Requirement	Release 1	Comments
A86	Lawful interception.	Y	

4.5.5 Unrestricted access by users to different service providers

Req	Requirement	Release 1	Comments
A87	Unrestricted access by users to different service providers.	Y	

Annex A (normative): Unordered List of Consolidated NGN Management Requirements

This annex provides a single unordered list of numbered consolidated requirements. This list is the result of an analysis of the requirements identified in annex B.

Column 1 provides a unique requirement number.

Column 2 provides a link to the unordered list of requirements in annex B.

Column 3 identifies if the requirement is applicable to NGN Release 1 [2].

Column 4 identifies which clause the requirement has been mapped to in clause 4:

- 4.1 Customer Centric;
- 4.2 Business Vision;
- 4.3 Technology Requirements;
- 4.4 Operator requirements;
- 4.5 Regulatory requirements.

Column 5 provides comments and additional information.

Req	Annex B Req#r	Requirement	Release 1	Categorized in paragraph	Comments
A1	B1	Management of User Equipment (including configuration and downloading of applications and QoS).	Y	4.3.9	
A2	B2 B3 B5 B6	Management of end to end connectivity (Transport).	Y	4.3.7, 4.3.1	
A3	B4	Support of multiple access technologies (including, as a minimum, Integrated access devices (IAD), DSL and WLAN access, gigabit Ethernet metro core networks).	Y	4.3.6	
A4	B7 B8	Management of Session Control, Media Control and Bearer Control.	Y	4.3.3	
A5	B9	Management of Mobility.	Y (see note 1)	4.1.10, 4.5.2	Only nomadism required for release 1 (i.e. no support for hand-over of communications sessions between access networks).
A6	B10	Management of Personalization of Services.	Y	4.1.2, 4.2.4	
A7	B11	Management of Location and context Services.	Y	4.2.4	
A8	B12	Management of NGN Service Layer entities.	Y	4.3.2	
A9	B13	Supporting the management Parlay v 4.0 APIs.		4.2.2	
A10	B14	Management of storage distribution of applications and content using Digital Rights.		4.2.1	These shall cover access control, user and content owners policy and support for creating accounting records for user by users and content application providers of users and management.
A11	B15	Management of end to end VPN solutions.	Y	4.2.3	

Req	Annex B Req#r	Requirement	Release 1	Categorized in paragraph	Comments
A12	B16 B17 B91 B92	Management of IP QoS across technical sub-domains and between operators.	Y	4.4.1	Interfaces between operators shall not assume a single end to end technical solution for IP QoS.
A13	B18	Support the use of protection mechanisms in the Access, core, metro, backhaul and with OLOs.		4.4.1	
A14	B19	Support national emergency services and international Emergency Telecommunications Services.		4.5.1	
A15	B20	Management systems shall be capable of supporting customer segmentation in the 10 000's.		4.1	
A16	B21 B43 B44 B45	Management of User Profile information shall allow distribution amongst networks, OSS, admin domains and end user terminals (user equipment).	Y	4.1.6, 4.1.8	
A17	B22	Processes for distribution and synchronization of User Profile information shall enforce policies set by regulation, applicable data protection laws, users and operators.	Y	4.5.3	
A18	B23	Service Detail Records and Product codes need to be managed in the 1 000's.		4.2.2	
A19	B25 B33 B40 B41 B102	Management processes shall support flexible, transport technology agnostic, service creation environments.	Y	4.4.5	
A20	B26 B38 B40 B101 B105 B115	Management processes shall support and automate Product Lifecycle Management.	Y	4.2.5, 4.4.5	
A21	B27	Management processes shall support the User Access control and trust Processes.	Y	4.1.1, 4.5.2	
A22	B28	Management processes shall support dynamic association of access points with User Profile and Subscription information.	Y	4.1.8	
A23	B29	Management processes shall support "off-net" presentation by users.		4.1.1	
A24	B30	Support multiple billing models, including billing on behalf of others.	Y	4.1.7, 4.2.1	
A25	B30	products codes shall not be tied 1 to 1 with specific tariffs.	Y	4.1	
A26	B31 B94	Value Chain technology Support for varying and changing business models shall be supported.	Y	4.2.1	
A27	B31	For B2B, the use of main stream e-commerce solutions shall be supported.	Y	4.2.1	
A28	B33 B34 B35 B36	The service creation process shall support the creation of (software) components whose services are exposed via contracts.	Y	4.4.5	
A29	Objective 8	The components created by the service creation process shall use a common information model.	Y	4.4.5	
A30	B37	The service creation process shall support a directory (or trading) feature for contracts in order to facilitate the design of software from existing (Off the Shelf) components.	Y	4.4.5	

Req	Annex B Req#r	Requirement	Release 1	Categorized in paragraph	Comments
A31	B39 B104	Providing the management capabilities which will enable organizations offering NGN end user service improvements including customer self service (e.g. provision of service, reporting faults, online billing reports), SLA Enforcement.	Y	4.4.3, 4.4.5	
A32	B40	Enable reusability by definition of building blocks, which describe and represent unitary service features or network features.	Y	4.4.5	
A33	B41 B42 B48 B50 B52	Management of the subscription related aspects of the user profile (subscription profile) including ownership of components.	Y	4.1.3	Subscription profile components will be needed for: data related to subscription identification and numbering. E.g. private identity, public identity, registration status; data related to roaming; data related to authentication and ciphering; data related to SPOA selection information; data related to applications and service triggers.
A34	B46	Control the capabilities that need to be offered to Business to Business (B2B) trading partners, such as value add service providers.		4.2.1	
A35	B50	Subscription management shall be able to control the ownership of components common to the user profile and the subscription profile.	Y	4.1.3	
A36	B54	Modifications by the subscription management to subscription profile components shall be recorded in an historical log.	Y	4.1.3	
A37	B55	Management shall provide a processes to support a customer wishing to check their subscription configuration.		4.1.1	
A38	B57	It shall be possible to replicate and distribute the subscription profile components following rules established and defined by subscription management feature.	Y	4.4.2	
A39	B58	Interfaces between trading partners shall meet the commercial and legal standards required for the business to business transactions.	Y	4.2.1, 4.5.3	Focus on Accounting and Billing for R1.
A40	B59	Interfaces supporting relationships between organizations shall use mainstream e-commerce technology methods.	Y	4.2.1	
A41	B60	To claim to be NGN compliant management interfaces shall be open and use industry standard solutions.	Y	4.4.6	
A42	B62 B53 B56 B97	Access to customer information shall only be permitted in an authorized and secure manner.	Y	4.1.3, 4.5.2	

Req	Annex B Req#r	Requirement	Release 1	Categorized in paragraph	Comments
A43	B63 B97 B61 B97 B106	Secure mechanisms shall be available for the transfer of data (e.g. customer data) to, from or between authorized entities and shall be appropriate to the level of confidentiality of the data, the endpoints of the transfer and the routes that are available for the transfer of the data. The owner of the data, normally the body storing the master copy of the data, shall be responsible for applying the appropriate level of security to the transfer of the data.	Y	4.5.2	
A44	B64 B97	Before any transfer takes place, it shall be possible for the sender of the data to verify the identity of the recipient.	Y	4.5.2	
A45	B65 B97	It shall be possible for the recipient of data to identify the sender.	Y	4.5.2	
A46	B66 B97	It is permissible for either the sender or recipient of data to employ the services of a third party, known to, and trusted by, both in order to provide authentication of identity.	Y	4.5.2	
A47	B67 B97	The validity of an authentication of identity shall, if required, be subject to a maximum time limit.	Y	4.5.2	
A48	B68 B97	It shall be possible for the sender of data to render the data to be unreadable by any party not authorized to receive it.	Y	4.5.2	
A49	B69 B97	It shall be possible for the recipient of data to detect whether the sender has made any change to the data subsequent to its transmission.	Y	4.5.2	
A50	B70 B97	The security mechanisms shall provide verification that the data has been sent by the sender and received by the recipient (non-repudiation).	Y	4.5.2	
A51	B71 B97	It shall be possible for the sender and/or the recipient to create an audit log of all data transfer transactions of a specified type, provided that this requirement is made known before any transfer takes place.	Y	4.5.2	
A52	B72 B97	Transaction security for the change of data should be available in order to ensure the consistent change of data at different locations.	Y	4.5.2	
A53	B73 B97	Management features will need to bridge between the NGN security functions and the security used in mainstream e-commerce solutions such as those in ebXML.		4.5.2	
A54	B74	Management shall fulfil local privacy regulations.	Y	4.5.3	
A55	B76	To be able to discover the current policy decision and policy enforcement points for a given access segment/given customer.	Y	4.4.6	
A56	B77	To be able to validate the current policy enforced within the network domain.	Y	4.4.6	
A57	B78 B80	To be able to discover the policy being enforced in an adjacent service or customer domain.		4.4.6	
A58	B79 B82	To be able to validate that the policies being enforced in an adjacent service or customer domain are compatible.		4.4.6	

Req	Annex B Req#r	Requirement	Release 1	Categorized in paragraph	Comments
A59	B81	To be able to discover limitations imposed by the terminal (user equipment) that the user has connected. (Analogue phone, IP Phone, PC).	Y	4.1.2, 4.4.6	
A60	B83	Discovery of the configuration (physical and logical) of an access segment including the source of configuration data.	Y	4.1.2, 4.4.6	To be able to discover which ingress node applies for a particular endpoint or access segment and where admission control is applied. And how it is configured for that endpoint or access segment. To be able to discover the information source used to configure the above and discover the data it contains. To be able to compare the two. To be able to discover the current loading of ingress/admission elements and of queues. Where appropriate, to be able to discover alternate/fallback entities and equipment.
A61	B84	Discovery of the configuration (physical and logical) of the signalling routing.	Y	4.4.6	To be able to discover the two way routing of signalling between an endpoint and its call control entity, and identify any intermediate Gateways and Interworking Functions, including which network nodes they are hosted on. To be able to discover the current configuration of "Virtual circuits" e.g. MPLS. To be able to discover the current transport network route topology. To be able to use this information to infer the routing of media streams (both directions) for given endpoints, customers, service types.
A62	B85	To be able to discover which egress node applies for specific called and calling party pairs.	Y	4.4.6	Note that where alternate routings apply there can be more than one possible egress node. To be able to discover the type and configuration of these egress nodes, especially any policy enforcement rules and related measurements. To be able to discover the current loading of egress elements and of their queues (see note 2).

Req	Annex B Req#r	Requirement	Release 1	Categorized in paragraph	Comments
A63	B86	Discovery of the configuration (physical and logical) of the core network.	Y	4.4.6	To be able to discover which instances of call controller; intermediate gateways/IWF; service quality management entities. currently apply for a particular endpoint or access segment, and which physical equipment they are currently hosted on. To be able to discover configuration data from them related to that endpoint or access segment. More work is needed to list out the key configuration information needed. However, it includes: records of improper call terminations and reason codes; call usage records; quality criteria currently applicable for endpoint, customer, service type. Both measurements and rules; in mobile IP, identification of past and present Foreign Agents and their transport addresses; see also addressing clause.
A64	B87 B75	From the unique identifier (E164, ENUM etc.), to be able to trace, where applicable, current: log on name and password; network endpoint IP address and hardware address; terminal (user equipment) IP address and hardware address. And the reverse.	Y	4.4.6	To be able to identify the functional entities (e.g. DNS, DHCP, and LDAP Server) responsible for: network log on; issue of IP address; configuration of terminal/soft client e.g. from user profile, for network capability; resolution of called party unique identifier e.g. E164, ENUM to transport address(es). And the physical equipment they are hosted on. To be able to discover current configuration data from those entities. Where appropriate, to be able to discover alternate/fallback equipments and entities. Where a "chain of responsibility" exists, to be able to discover the next in line.
A65	B88 B93	Fault management functions (including Alarm Surveillance) and associated managed objects shall be applicable to all NGN entities.		4.4.6	Fault Management is outside the scope of NGN OSS Release 1.
A66	B89	Under Crisis situations (either network related or external) the NGN shall continue to provide essential management information and accept management controls.	Y	4.4.6	
A67	B90	NGN Management will exploit wherever possible the business and service processes as defined by the ITU-T and TeleManagement Forum (TMF) i.e. ITU-T Recommendation M.3050 [3].	Y	4.4.6	
A68	B90	NGN Management will exploit wherever possible the management communication protocols and information bases already defined.	Y	4.4.6	

Req	Annex B Req#r	Requirement	Release 1	Categorized in paragraph	Comments
A69	94bis	Bill limitations It can be necessary to protect users from bills of unexpected amounts. Further it may be necessary to protect users from misuse of their accounts, and to protect operators from misuse of services.		4.1.7	
A70	B95	Secure billing administration.	Y	4.5.2	
A71	95bis	Authorization control (e.g. via black lists) to prevent fraud.	FFS	4.5.2	
A72	96	Customer Hotline.		4.1.1	
A73	B96bis	Support Security related reports to the user.		4.5.2	
A74	B98	Contractual agreements relating to security issues can be included in the roaming agreement between two operators.		4.2.2	
A75	B99	Contractual agreements between service providers and subscribers relating to security issues shall be included in the conditions for the subscription.	Y	4.5.2	
A76	B100	A secure subscription process to restrict subscription fraud.	Y	4.5.2	
A80	B109	Allowing an enterprise and/or an individual to adopt multiple roles in different value networks and also multiple roles within a specific value network (e.g. one role as a retail Service Provider and another role as a wholesale Service Provider) (ITU-T Recommendation M.3050 [3]).	Y	4.2.1	
A81	B111	Allowing the management of hybrid networks comprising NGN and non-NGN (e.g. PSTN, cable network) resources.	Y		
A82	B112	Integrating an abstracted view on Resources (network, computing and application), which is hiding complexity and multiplicity of technologies and domains in the resource layer.	Y	4.3.2	
A83	B113	Supporting the collection of charging data for the network operator regarding the utilization of resources in the network either for later use by billing processes (offline charging) or for near-real time interactions with rating applications (online charging).	Y	4.1.7	
A84	B114	Unified service characteristics for the same service as perceived by the user.	Y	4.4	
A85	B117	Support TISPAN Release 1 Services.	Y	4.2.3 4.3.4	
A86	B119	Lawful interception.	Y	4.5.4	
A87	B120	Unrestricted access by users to different service providers.	Y	4.5.6	
A88	B121	Support a variety of identification schemes.	FFS	4.3.8	
A88	B118	Perfect touch and zero fall-out.		4.4.4	
A89	B116	Single sign on.		4.1.9	
NOTE 1: There are significant impacts in the security and personalization aspects of the services. NOTE 2: Egress means here egress from the service provider/network operators Administrative Domain.					

Annex B (informative): List of NGN Management Requirements before consolidation

This annex provides an unordered list of numbered requirements and identifies the source of the requirement. New requirements will be added to the end of the list and allocated a new number as they are agreed.

B.1 Requirements derived from the NGN Management OSS Vision

The following requirements are derived from TR 188 004: OSS NGN Vision [1].

Req#r	Requirement
B1	Terminal Management Interfaces. Standardized processes and NML-EML interfaces shall be defined for the management of terminals and the configuration and downloading of applications to NGN terminals. These shall cover the requirements of configuration and assurance processes including QoS.
B2	Connectivity management. Standardized processes and NML-EML interfaces (Q3 equiv) shall be defined for the management of end to end connectivity paths.
B3	Connectivity management. Standardized processes and NML-EML interfaces for connectivity management shall be supported either by management or control plane (signalling control management).
B4	Connectivity management. Shall cover as a minimum, Integrated Access Devices (IAD), DSL and WLAN access, gigabit Ethernet metro core networks using DiffServ and MPLS.
B5	Connectivity management to OLO networks. Standardized processes and OSS-OSS interfaces (X interface equiv.) shall be defined for the Strategy Infrastructure and Product (SIP-eTOM) groups and the Operations Group of the eTOM.
B6	Connectivity management IPv6. Standardized processes and NML-EML interfaces shall be defined for management of IPV6 transport.
B7	Signalling management Standardized processes and NML-EML interfaces shall be defined for management of IP Signalling mechanisms including, DIFFSERV, MPLS, BGP4+, OSPF, Note this list needs to be qualified with RFC numbers and it is likely that IETF MIBs and TMF IPNM specs will partially cover this requirement.
B8	Traffic management: Standardized processes NML-EML and OSS-OSS interfaces shall be defined for management of Signalling in A multi-service IP network carried voice and multimedia services.
B9	Mobility: Standardized processes NML-EML and OSS-OSS interfaces shall be defined for management of Mobility services. These shall be aligned with standards deployed in 2G 2.5G and emerging 3G services. Note there are significant impacts in the security and personalization aspects of the services.
B10	Intelligence personalization Standardized processes NML-EML and OSS-OSS interfaces shall be defined for management of Personalization service (I.e. 3GPP VHE and HSS).
B11	Intelligence location/ context Standardized processes NML-EML and OSS-OSS interfaces shall be defined for management of Location and context service.
B12	Standardized processes NML-EML and OSS-OSS interfaces shall be defined for management of Voice and multimedia using SIP Servers and media gateways.
B13	Intelligence Parlay Standardized processes SML-NML and OSS-OSS interfaces shall be defined for supporting the management Parlay v 4.0 APIs.
B14	Intelligence Contents Standardized processes SML-NML and OSS-OSS interfaces shall be defined for management of storage distribution of applications and content using Digital Rights These shall cover access control, user and content owners policy and support for creating accounting records for user by users and content application providers of users and management.
B15	Intelligence VPN Standardized processes SML-NML and OSS-OSS interfaces shall be defined for supporting the management of end to end VPN solutions.
B16	QoS Standardized processes and NML-EML and OSS-OSS interfaces shall be defined for supporting the management of IP QoS across technical sub-domains and between operators.
B17	QoS Standardized processes and OSS-OSS interfaces between operators shall not assume a single end to end technical solution for IP QoS signalling. Assumption shall be restricted to technical capabilities that are required at the interconnect points.
B18	Availability backup Standardized processes NML-EML and OSS-OSS interfaces between operators shall support the use of protection mechanisms in the Access, core, metro, backhaul and with OLOs.
B19	Availability emergency services Standardized processes NML-EML and OSS-OSS interfaces between operators shall support the ITU Emergency Telecommunications Service.

Req#r	Requirement
B20	Service and Network Management systems shall be capable of supporting customer segmentation in the 10 000's.
B21	Management of User Profile information shall allow distribution amongst networks, OSS and end user terminals.
B22	Processes for distribution and synchronization of User Profile information shall enforce policies set by regulation, applicable data protection laws, users and operators.
B23	Service Detail Records and Product codes need to be managed in the 1 000's.
B24	*<Duplicate>*
B25	Management processes shall support service creation environments.
B26	Management processes shall support and automate Product Lifecycle Management integrated in to OSS for Fulfilment Assurance and Billing.
B27	Management processes shall support the configuration and operations of User Access control and trust Processes that work access multiple access technologies.
B28	Management processes shall support dynamic association of access points with User Profile and Subscription information.
B29	Management processes shall support "off-net" presentation by users. User profile and subscription information shall be dynamically associated with access points.
B30	Tariffs for products shall be set by a combination of the products, the User/Customer and the subscription tariff plan. Product codes should not assume a single user independent tariff and products codes shall not be tied 1 to 1 with specific tariffs.
B31	Value Chain technology Support for varying and changing business models shall be supported. Use of main stream e-commerce solutions shall be supported.
B32	revenue sharing Billing processes, NML and OSS-OSS interfaces shall support models. Support for Billing on Behalf of Others Sponsorship models free trials discount certificates - transferable, advertising and competitions.

B.2 Requirements to Support Service Creation

The following requirements are derived from contributions submitted to ETSI TISPAN WG8.

Req#r	Requirement
B33	The service creation process shall support the creation of (software) components independent of the underlying CCV technology, i.e., a given service shall be able to work on any given CCV that meets the TM Forum NGOSS requirements.
B34	The service creation process shall support the creation of components whose services are exposed via contracts. Each contract definition shall have clearly stated pre-conditions and post-conditions, and a summary of the service provided by the contract.
Objective 1	The contract descriptions shall follow the structure stated in TMF 053B, NGOSS Architecture Technology Neutral Specification - Contract Description: Business and System Views.
B35	Software components shall be designed to allow for the external orchestration of contracts in support of various business processes.
B36	For a given set of software components, it should be possible to support different business processes by using various subsets of the offered contracts in a specific flow with appropriate parameter settings.
B37	The service creation process shall support a directory (or trading) feature for contracts in order to facilitate the design of software from existing (Off the Shelf) components.
Objective 2	The components created by the service creation process shall use a common information model. [Note: This may be difficult if COTS software is to be used, since it is hard if not impossible to legislate a common information model. The TM Forum SID model would be a good choice if one could legislate a common information model.]
Objective 3	With suitable adaptation, the service creation process shall support the incorporation non-compliant software entities, where non-compliant refers to software entities that do not support all of the requirement listed previously. This could be accomplished by adding a contract adaptation layer over the native interfaces offered by the legacy software entities. Of course, the possibility of upgrading legacy software may not always be practical in terms of time and cost.
B38	The service creation environment must be sufficiently flexible, ubiquitous, and cost-effective to enable a service provider to define, fulfil, assure, and bill a new service without going through the operations support system (OSS) development cycle.

Req#r	Requirement
B39	The operational requirements for the service creation architecture include the following: Customer self-servicing and other customer care functions for higher-level services. Ordering Interface and associated business process. Support for activation and validation of the service needs to be automatic, using methods such as rule engines that can realize the actual deployment and management of a service instance from the abstract service description. The service creation process needs to enable flows from servers to the billing SMS. SLA Enforcement.
B40	A well-designed Service Model is the basis for effective, flexible service creation. A service model provides multiple benefits such as: Enable innovation in new services, without incurring the full development cycle for operations support functionality. Abstract from network technology, where possible, which enables new services to be created without undue dependency on network technology details. Enable reusability by definition of building blocks, which describe and represent unitary service features or network features. New services can be designed by aggregation of existing blocks and/or creation of new ones.
B41	A service model should facilitate all of the following: Achieve rapid, cost effective OSS support as new services are introduced, by efficiently mechanizing the realization of the service model. The service creation model defines services in terms of process needs and information flows. This definition provides rule-based sequencing of the actions related to fulfilment, assurance, and billing Specify and track the dependencies of services on underlying network and service components. Measure and quantify customer satisfaction in terms of the services they receive. Manage a large number of new services and SLAs (internal/external). Be a scalable approach in terms of network impact and operations impact.
NOTE 1: In any event, some form of standard contract definition should be used. TMF 053B seems to be a reasonable choice.	
NOTE 2: This may be difficult if COTS software is to be used, since it is hard if not impossible to legislate a common information model. The TM Forum SID model would be a good choice if one could legislate a common information model.	

B.3 Requirements derived from TIPHON Management TR

The following requirements are derived from TS 132 101 [4], TS 132 102 [5] and TR 101 303 [6].

Req#r	Requirement
B42	Subscription management shall provide the management of the subscription related aspects of the user profile (subscription profile).
B43	Subscription management shall support the replication and distribution of subscriber profile components (fragments of the user profile) across administrative, network and systems domains.
B44	Subscription management shall control of the synchronization and distribution of user profile components across administrative, network and systems domains.
B45	Subscription management shall control the capabilities required by the customer care operations for the control and modification of user profile information.
B46	Subscription management shall control the capabilities that need to be offered to Business to Business (B2B) trading partners, such as value add service providers.
B47	The primary area where subscription profile components are stored is in the home network in the home network registration function. This function will be used by the network for distribution and replication of this data in other entities.
B48	Subscription management shall allow for the creating, reading, updating and deleting of subscription profile data in the home network registration function.
B49	Subscription management shall support the data structures and organization described in UMTS user profiles/service profiles.
B50	Subscription management shall be able to control the ownership of components common to the user profile and the subscription profile.
B51	Subscription management shall manage subscription profile components within the home network.
B52	Subscription profile components will be needed for: data related to subscription identification and numbering. E.g. private identity, public identity, registration status; data related to roaming; data related to authentication and ciphering; data related to SPOA selection information; data related to applications and service triggers.

Req#r	Requirement
B53	Requirements on Authentication: - subscription management shall be able to create, read, modify and delete data about a user in an authentication system.
B54	Modifications by the subscription management to subscription profile components shall be recorded in an historical log.
B55	Subscription management shall provide a process to support a subscriber wishing to check their subscription configuration.
B56	Authentication of a subscriber shall be provided to prevent anyone other than the subscriber or an authorized person from gaining access to their subscription profile.
B57	It shall be possible to replicate and distribute the subscription profile components following rules established and defined by subscription management feature.
B58	Interfaces between trading partners shall meet the commercial and legal standards required for the business to business transactions.
B59	Interfaces supporting relationships between organizations shall use mainstream e-commerce technology methods.
B60	To claim to be NGN compliant management interfaces between Subscription management components within an organization shall be open and use industry standard solutions (e.g. CORBA, CMIP, XML, OSSJ, or SNMP).
B61	Secure mechanisms shall be available for the transfer of subscription profile components to, from or between authorized entities.
B62	Access to customer information shall only be permitted in an authorized and secure manner.
B63	The secure mechanisms to be applied shall be appropriate to the level of confidentiality of the data, the endpoints of the transfer and the routes that are available for the transfer of the data. The owner of the data, normally the body storing the master copy of the data, shall be responsible for applying the appropriate level of security to the transfer of the data.
B64	A Before any transfer takes place, it shall be possible for the sender of the data to verify the identity of the recipient.
B65	B It shall be possible for the recipient of data to identify the sender.
B66	C It is permissible for either the sender or recipient of data to employ the services of a third party, known to, and trusted by, both in order to provide authentication of identity.
B67	D The validity of an authentication of identity shall, if required, be subject to a maximum time limit.
B68	E It shall be possible for the sender of data to render the data to be unreadable by any party not authorized to receive it.
B69	F It shall be possible for the recipient of data to detect whether the sender has made any change to the data subsequent to its transmission.
B70	G The security mechanisms shall provide verification that the data has been sent by the sender and received by the recipient (non-repudiation).
B71	H It shall be possible for the sender and/or the recipient to create an audit log of all data transfer transactions of a specified type, provided that this requirement is made known before any transfer takes place.
B72	I Transaction security for the change of data should be available in order to ensure the consistent change of data at different locations.
B73	Management features will need to bridge between the NGN security functions and the security used in mainstream e-commerce solutions such as those in ebXML.
B74	Management shall fulfil local privacy regulations.
B75	To be able to discover from the E164 number the network endpoint and access segment that currently services the customer.
B76	To be able to discover the current policy decision and policy enforcement points for a given access segment/given customer.
B77	To be able to validate the current policy enforced within the network domain.
B78	To be able to discover the policy being enforced in an adjacent service domain.
B79	To be able to validate that the two are compatible.
B80	To be able to discover policy being enforced in the customer owned network.
B81	To be able to discover limitations imposed by the terminal that the user has connected. (Analogue phone, IP Phone, PC).
B82	To be able to validate that this and own network policy are compatible.
B83	Admission: To be able to discover which ingress node applies for a particular endpoint or access segment and where admission control is applied. And how it is configured for that endpoint or access segment. To be able to discover the information source used to configure the above and discover the data it contains. To be able to compare the two. To be able to discover the current loading of ingress/admission elements and of queues. Where appropriate, to be able to discover alternate/fallback entities and equipment.

Req#r	Requirement
B84	Transport And routing: To be able to discover the two way routing of signalling between an endpoint and its call control entity, and identify any intermediate Gateways and Interworking Functions, including which network nodes they are hosted on. To be able to discover the current configuration of "Virtual circuits" e.g. MPLS. To be able to discover the current transport network route topology. To be able to use this information to infer the routing of media streams (both directions) for given endpoints, customers, service types.
B85	Egress To be able to discover which egress node applies for specific called and calling party pairs. Note that where alternate routings apply there can be more than one possible egress node. To be able to discover the type and configuration of these egress nodes, especially any policy enforcement rules and related measurements. To be able to discover the current loading of egress elements and of their queues.
B86	Service control To be able to discover which instances of call controller; intermediate gateways/IWF; service quality management entities. currently apply for a particular endpoint or access segment, and which physical equipment they are currently hosted on. To be able to discover configuration data from them related to that endpoint or access segment. More work is needed to list out the key configuration information needed. However, it includes: records of improper call terminations and reason codes; call usage records; quality criteria currently applicable for endpoint, customer, service type. Both measurements and rules; in mobile IP, identification of past and present Foreign Agents and their transport addresses; see also addressing clause.
B87	From the unique identifier (E164, ENUM etc.), to be able to trace, where applicable, current: log on name and password; network endpoint IP address and hardware address; terminal IP address and hardware address. And the reverse. To be able to identify the functional entities (e.g. DNS, DHCP, and LDAP Server) responsible for: network log on; issue of IP address; configuration of terminal/soft client e.g. from user profile, for network capability; resolution of called party unique identifier e.g. E164, ENUM to transport address(es). And the physical equipment they are hosted on. To be able to discover current configuration data from those entities. Where appropriate, to be able to discover alternate/fallback equipments and entities. Where a "chain of responsibility" exists, to be able to discover the next in line.
	Fault management
B88	Fault management Fault management functions and associated managed objects shall be applicable to all NGN entities (gateways with various PSTN interfaces, call control entities - gatekeepers, media gateway controllers or call agents, MCU, terminals - IP telephones, residential gateways, etc.). In order to meet this requirement, the work should primarily be based on the functional entities of the IP telephony plane Management functions shall be independent of signalling protocols (IETF SIP/MGCP/MEGACO, ITU-T Recommendation H.323/H.248, etc.). This implies a common terminology to reference class members and potential some mapping work (for e.g., when logging events on a particular call, the call identifier parameter should be mapped to its equivalent parameters in all sig protocol: SIP Call-ID general-header field, H.225.0 CallIdentifier, MGCP CallId, etc.). In its first release, information models and TIPHON network management specifications shall be implementable with currently available management protocols. For each management function, the level of requirement must be clearly stated for each TIPHON release; we will define a set of mandatory/optional alarm events and even log attributes for each TIPHON network entities and for each TIPHON releases (alarm perceived severity, alarm status, probable cause, alarm thresholds, etc.). Alarm Severity Assignment profiles should be included. The states of managed objects shall follow the general definitions of X.731 (operational state: disabled | enabled; administrative state: locked | shutting down | unlocked; usage state: idle | active | busy).
B89	Under Crisis situations (either network related or external) the NGN shall continue to provide essential management information and accept management controls.
B90	the TNM will exploit wherever possible: the business and service processes as defined by the TeleManagement Forum (TMF); the management communication protocols and information bases already defined by IETF and ITU-T.

Req#r	Requirement
B91	In order to deliver the intended end-to-end speech transmission quality in NGN systems, transmission planning should be performed during the design phase of NGN related equipment. It is not sufficient to design equipment or networks just along the requirement limits of the respective NGN class. Any variation of transmission parameters should only be judged on the basis of E-model calculations for critical end-to end connections. Any assumption whether or whether not a specific parameter variation will be perceived by the user should always be based on E-model calculations. Special care should be taken with devices which dynamically vary one or more transmission parameters, e.g. Automatic Level Control (ALC) devices; experiences with such devices have shown that they have the potential to impact end-to-end speech transmission quality, severely.
B92	After NGN equipment and networks have been designed, planned and rendered operative in compliance with one the NGN QoS classes it might - nevertheless - occur that users complain about too low speech quality. In such cases, it is very important to be able to carry through a diagnosis of end-to-end speech transmission performance. For that it will be needed to keep track of all parameter changes (e.g. of send and receive loudness rating) carried out either automatically or by user interaction. This should be considered already during the design phase of NGN equipment and networks, e.g. by providing tools to set parameters back to default values or by providing a log file function.
92bis	Even if a specific NGN system has been operated for some time at the desired level of customer satisfaction it will be required to continuously monitor and check the end-to-end speech transmission quality. Verification will require access to the actual settings of all major transmission parameters - including those which were accessible to the user.
B93	Alarm surveillance requirements for NGN Alarm surveillance includes alarm reporting, alarm summary, alarm severity assignment profiles, alarm indication management and log control. The definition of alarm surveillance used in this TD is based on ITU-T Recommendation Q.821. From TR 101 303 [6] alarm surveillance functions are used to monitor NEs about events or conditions: the event data is generated by a NE upon the detection of an abnormal condition. Examples of such events are detection of transmission data errors, the violation of a performance threshold, and the detection of faulty equipment; event data can be reported at the time of occurrence, logged for future access, or both. The purpose of this clause is to identify the requirements for NGN entities in NGN release 3, in particular: The level of requirement for each alarm surveillance functions: alarm reporting, alarm summary, alarm event criteria (severity assign.), alarm indication management, log control; Categories of alarm event types for NGN systems: communications alarm type, quality of service alarm type, Processing error alarm type, Equipment alarm type, Environmental alarm type; Event information: Probable causes (define specific list of causes for NGN NE, perceived severity (define severity assignment profile guidelines for each type of VoIP NE), etc.; Log control: event logging including remote logging requirements.
B94	Service Level Interconnection: The agreement for service level interconnection will need to specify (TS 101 878: a common base service application or applications that will be inter-worked; common standardized service capabilities at the service level together with the values of any particular parameters (e.g. a form of profile); any additional common but non-standardized functionality at the service level; a common naming scheme with a co-ordinated system for allocating names to users; a service provider identity that the roaming user will use at registration time; an agreed naming scheme for identifying each network (for routing, it is necessary to determine the home network name from the called user name); the technology (protocols) for implementing the interconnection. together with the relevant quality of service values and the commercial arrangements. Roaming level interconnection: The agreement for roaming level interconnection will need to specify: service capabilities needed for the roaming users along with parameters that may be prescribed or signalled during service usage; a service provider identity that the roaming user will use at registration time; service applications that are to be resolved locally (such as emergency calls); the technology (protocols) for implementing the interconnection. together with the relevant quality of service values and the commercial arrangements. Transport level interconnection: The agreement for transport level interconnection will need to specify: any non-standardized functionality at the transport level that is the subject of innovation; technology (Protocols) e.g. IP or ATM used to implement the inter-domain transport and signalling. together with the relevant quality of service values and the commercial arrangements.

Req#r	Requirement
B 94bis	Bill limitations It can be necessary to protect users from bills of unexpected amounts. Further it may be necessary to protect users from misuse of their accounts, and to protect operators from misuse of services. Different methods, or combinations of methods, are possible to realize this requirement: absolute bill limitation: when a subscriber opens an account, there can be an option to set a credit limit on the account. The total amount of the current bill of the subscriber may be checked at call set-up. A policy can be implemented about the acceptance or not of the call in case of exceeding bill limit. This can limit damage if abuse takes place. bill limitation with respect to time: another possible measure would be to limit the bill with respect to time. Thus, the credit limit may be on a day-by-day basis, on a weekly basis, or provide an overall limit. That means, if e.g. a limit per week is agreed and this limit is exceeded (at call set-up or during a call), the user access would be blocked for the rest of the week. origin and destination limits: another security measure may be for certain accounts (for new or less trustworthy subscribers) to limit the destinations of calls. The limit may be within a given area, within the country, or even only to a specified destination address. Likewise, a limit may be put on the caller's location for outgoing calls.
B95	7.8.2 Secure billing administration The billing administration may have to consider security very carefully. Billing data and related personal data can be stored, processed, and transmitted in such a way that user privacy and data integrity are guaranteed. Itemized bills may be a means for the NGN subscriber to check the correctness of the billing. Thus, the billing administration can send to the user an explained bill with the called numbers and split in different part like regional calls, national calls, and international calls. However, to avoid conflicts with privacy requirements, the subscriber can also have the possibility to get only summarized bills.
95bis	7.8.3 Subscriber and terminal management Limiting the access to services by means of subscription restriction or equipment restriction can reduce otherwise unacceptable risks. This can be achieved in a number of ways such as by the use of black lists to identify rogue subscribers or rogue equipment. Service may be denied to subscribers or equipment that appears on such a black list. A white list gives unrestricted access to subscribers and equipment (within any limits set by their service profile). Intermediate variants of these lists may be maintained to track potential bad debt or potential fraud.
B96	7.8.4 Customer hotline A customer hotline can be provided by the operator in order to answer users' questions like "My service does not work", "I have received too high a bill". This service may be useful for security reasons in case of theft or loss of terminal or in case of unexpected behaviour of the service of a subscriber where specific procedures should be implemented. In case of theft or loss of terminal, this procedure can be: location of the stolen or lost terminal in order to find it; block incoming and outgoing calls; put the NGN number on a black list; no charging for the subscriber of calls performed after the report of the theft; and de-registration of the terminal after location.
B96bis	Security related reports to the user Recording and presentation of information about actions performed by users in the system (event reporting) may often function as a supporting security service. (Users' knowledge of this fact may in turn work as a deterrent factor). Announcements must be carefully designed to enlighten users and third parties of the different states of their connection or relation with the operator/service provider. There can be a facility to inform NGN users about actions that affect their privacy and security or the charging. This information can be given on-line by announcements, special dial tones, or short messages. For example, the following information can be given to the users: "BILL LIMITATION EXCEEDED".
B97	Secure dialogue between operators Secure dialogues can consist of a mutual authentication procedure, a confidentiality service and a data integrity service on the communication link. It can be provided by: mutual authentication; link encryption; link data integrity; non-repudiation; and key management to support this.

Req#r	Requirement
B98	Contractual agreements between operators Contractual agreements relating to security issues can be included in the roaming agreement between two operators. When agreeing upon a roaming agreement two operators may define some security conditions. Those conditions can be: frequency of exchange of blacklists; liability of a visited network if it does not take the appropriate measures to stop a fraud; level of security audit guaranteed; follow the rules concerning the use of data an other network can get access to; co-operation in case of fraud; integrity of file transfer; minimum frequency of authentication to be performed for visiting NGN users; and, in case of dispute, one network operator should be able to provide the other network with every information related to billing.
B99	Contractual agreements between service providers and subscribers Contractual agreements relating to security issues shall be included in the conditions for the subscription. Security conditions to be agreed and signed by the subscriber could be: to follow the rules (as declared by the NGN service provider and adjoined to the subscription contract) regarding secure handling of his PIN if used to protect terminal; to report to the service provider immediately loss of terminal which might lead to fraud or misuse; to accept limitations of service with regard to agreed levels of credit control/bill limitation; and to accept limitations of service which the service provider later on may find necessary to introduce to protect the service as such against misuse or fraud.
B100	Secure subscription process A secure subscription process can restrict subscription fraud. A security policy may be applied to new subscribers in order to be to be confident in the ability and motivation of a subscriber to pay any bills. This may be achieved by authenticated or verified delivery of proofs of identity. It may be possible for subscriptions to be made available on a pre-paid (contract less) basis. It can be possible to inhibit service when the pre-payment is exceeded. The operator may restrict the number of subscriptions per subscriber.
NOTE 1: It seems to be necessary to define what is in a "policy" for the purposes of performance/quality management. NOTE 2: Egress means here egress from the service provider/network operators Administrative Domain.	

B.4 Requirements from NGN Release 1 Docs

The following requirements are derived from TR 180 001 [2].

Req#r	Requirement
B101	Providing the ability to manage, through their complete lifecycle, NGN system components, both physical and logical. This includes resources in the core network (including IMS), access networks, interconnect components and customer networks and their terminals.
B102	Providing the ability to manage NGN service components independently from the underlying NGN transport components and enabling organizations offering NGN end user services (potentially from different service providers) to build distinctive service offerings to customers.
B103	Providing the management capabilities which will enable organizations offering NGN end user services to offer customers the ability to personalize end user services and to create new services from service capabilities (potentially from different service providers).
B104	Providing the management capabilities which will enable organizations offering NGN end user service improvements including customer self service (e.g. provision of service, reporting faults, online billing reports).
B105	Developing a management architecture and management services which will enable service providers to reduce the time frame for the design, creation and delivery of new services.
B106	Supporting the security of management information, including customer and end user information.
B107	Supporting the availability of management services any place any time to any authorized organization or individual (e.g. access to billing records shall be available 24/7).
B108	Supporting eBusiness Value Networks based upon concepts of business roles (Customer, Service Provider, Complementor, Intermediary, Supplier (e.g. Equipment Vendor)) (ITU-T Recommendations Y.110 and M.3050 [3]).
B109	Allowing an enterprise and/or an individual to adopt multiple roles in different value networks and also multiple roles within a specific value network (e.g. one role as a retail Service Provider and another role as a wholesale Service Provider) (ITU-T Recommendation M.3050 [3]).
B110	Supporting B2B processes between organizations providing NGN services and capabilities.
B111	Allowing the management of hybrid networks comprising NGN and non-NGN (e.g. PSTN, cable network) resources.

Req#r	Requirement
B112	Integrating an abstracted view on Resources (network, computing and application), which is hiding complexity and multiplicity of technologies and domains in the resource layer.
B113	Supporting the collection of charging data for the network operator regarding the utilization of resources in the network either for later use by billing processes (offline charging) or for near-real time interactions with rating applications (online charging).

B.5 Additional requirements

The following requirements are derived from contributions to TISPAN WG8.

Req#r	Requirement	Release 1	Categorized in paragraph)	Comments
B114	Unified service characteristics for the same service as perceived by the user		4.4	
B115	Shortened product lifecycle		4.5	
B116	Single sign on		4.9	
B117	Support TISPAN Release 1 Services	Y	4.2.3 4.3.4	
B118	Perfect touch and zero fall-out		4.4.4	
B119	Lawful interception		4.5.4	
B120	Unrestricted access by users to different service providers		4.5.6	
B121	Support a variety of identification schemes	FFS	4.3.8	

Annex C (informative): Bibliography

IETF RFC 2916: "E.164 number and DNS".

ITU-T Recommendation E.164: "The international public telecommunication numbering plan".

ITU-T Recommendation Y.110: "Global Information Infrastructure principles and framework architecture".

ITU-T Recommendation H.323: "Packet-based multimedia communications systems".

ITU-T Recommendation H.248: "Gateway control protocol".

ITU-T Recommendation H.225.0: "Call signalling protocols and media stream packetization for packet-based multimedia communication systems".

ITU-T Recommendation X.731: "Information technology - Open Systems Interconnection - Systems Management: State management function".

ETSI TS 101 878: "Telecommunications and Internet Protocol Harmonization Over Networks (TIPHON) Release 4; Service Capability Definition; Service Capabilities for TIPHON Release 4".

History

Document history		
V1.1.1	September 2005	Publication