ETSI TS 132 101 V17.0.0 (2022-04)

**Digital cellular telecommunications system (Phase 2+) (GSM);
Universal Mobile Telecommunications System (UMTS);
LTE;
Telecommunication management;
Principles and high level requirements
(3GPP TS 32.101 version 17.0.0 Release 17)**

Reference
RTS/TSGS-0532101vh00

Keywords
GSM,LTE,UMTS

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 - APE 7112B
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° w061004871

Intellectual Property Rights

Essential patents

IPRs essential or potentially essential to normative deliverables may have been declared to ETSI. The declarations pertaining to these essential IPRs, if any, are 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 (https://ipr.etsi.org/).

Pursuant to the ETSI Directives including the ETSI IPR Policy, no investigation regarding the essentiality of IPRs, 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.

Trademarks

The present document may include trademarks and/or tradenames which are asserted and/or registered by their owners. ETSI claims no ownership of these except for any which are indicated as being the property of ETSI, and conveys no right to use or reproduce any trademark and/or tradename. Mention of those trademarks in the present document does not constitute an endorsement by ETSI of products, services or organizations associated with those trademarks.

DECT™, **PLUGTESTS™**, **UMTS™** and the ETSI logo are trademarks of ETSI registered for the benefit of its Members. **3GPP™** and **LTE™** are trademarks of ETSI registered for the benefit of its Members and of the 3GPP Organizational Partners. **oneM2M™** logo is a trademark of ETSI registered for the benefit of its Members and of the oneM2M Partners. **GSM**® and the GSM logo are trademarks registered and owned by the GSM Association.

Legal Notice

This Technical Specification (TS) has been produced by ETSI 3rd Generation Partnership Project (3GPP).

The present document may refer to technical specifications or reports using their 3GPP identities. These shall be interpreted as being references to the corresponding ETSI deliverables.

The cross reference between 3GPP and ETSI identities can be found under http://webapp.etsi.org/key/queryform.asp.

Modal verbs terminology

In the present document "**shall**", "**shall not**", "**should**", "**should not**", "**may**", "**need not**", "**will**", "**will not**", "**can**" and "**cannot**" are to be interpreted as described in clause 3.2 of the ETSI Drafting Rules (Verbal forms for the expression of provisions).

"**must**" and "**must not**" are **NOT** allowed in ETSI deliverables except when used in direct citation.

Contents

Foreword

This Technical Specification (TS) has been produced by the 3rd Generation Partnership Project (3GPP).

The contents of the present document are subject to continuing work within the TSG and may change following formal TSG approval. Should the TSG modify the contents of the present document, it will be re-released by the TSG with an identifying change of release date and an increase in version number as follows:

Version x.y.z

where:

x the first digit:

1 presented to TSG for information;

2 presented to TSG for approval;

3 or greater indicates TSG approved document under change control.

y the second digit is incremented for all changes of substance, i.e. technical enhancements, corrections, updates, etc.

z the third digit is incremented when editorial only changes have been incorporated in the document.-

1 Scope

The present document establishes and defines the management principles and high-level requirements for the management of PLMNs.

In particular, the present document identifies the requirements for:

- the upper level of a management system;
- the reference model, showing the elements the management system interacts with;
- the network operator processes needed to run, operate and maintain a network;
- the functional architecture of the management system;
- the principles to be applied to management interfaces.

The requirements identified in the present document are directed to the further development of management specifications as well as the development of management products. The present document can be seen as guidance for the development of all other Technical Specification addressing the management of PLMNs.

The present document does not provide physical architectures of the management system. These aspects are defined and discussed in more detail in TS 32.102 [101].

Verbal forms used to indicate requirements in the present document (e.g. "shall", "should", "may") are used in compliance with 3GPP specification Drafting Rules TR 21.801 [104].

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, edition number, version number, etc.) or non-specific.
- For a specific reference, subsequent revisions do not apply.
- For a non-specific reference, the latest version applies. In the case of a reference to a 3GPP document (including a GSM document), a non-specific reference implicitly refers to the latest version of that document *in the same Release as the present document*.

[1] ITU-T Recommendation M.3010 (2000): "Principles for a telecommunications management network".

[2] 3GPP TS 22.101: "Service aspects; Service Principles".

[3] 3GPP TS 32.111-1: "Telecommunication management; Fault Management; Part 1: 3G fault management requirements".

[4] IETF RFC 959: "File Transfer Protocol (FTP)"; October 1985, J. Postel, J. Reynolds, ISI. (Status: Standard).

[5] IETF RFC 783: "Trivial File Transfer Protocol (TFTP)"; rev. 2, June 1981, K.R. Sollins MIT. (Status: Unknown).

[6] IETF RFC 1157: "Simple Network Management Protocol (SNMP)": May 1990, J. Case, SNMP Research, M. Fedor, Performance Systems International, M. Schoffstall, Performance Systems International, J. Davin, MIT Laboratory for Computer Science. (Status: Standard).

[7] IETF RFC 2401: "Security Architecture for the Internet Protocol"; November 1998. (Status: Proposed Standard).

[8] The Object Management Group (OMG) "The Common Object Request Broker: Architecture and Specification", Revision 2.3, June 1999.
http://www.omg.org/technology/documents/vault.htm#CORBA_IIOP

[9] ... [12] Void

[13] ISO 8571-1 (1988): "Information Processing Systems - Open Systems Interconnection - File Transfer, Access and Management - Part 1: General Introduction".

[14] ISO 8571-2 (1988): "Information Processing Systems - Open Systems Interconnection - File Transfer, Access and Management - Part 2: Virtual Filestore Definition".

[15] ISO 8571-3 (1988): "Information Processing Systems - Open Systems Interconnection - File Transfer, Access and Management - Part 3: File Service Definition".

[16] ISO 8571-4 (1988): "Information Processing Systems - Open Systems Interconnection - File Transfer, Access and Management - Part 4: File Protocol Specification".

[17] ISO/IEC ISP 10607-1 (1995): "Information technology - International Standardized Profiles AFTnn - File Transfer, Access and Management - Part 1: Specification of ACSE, Presentation and Session Protocols for the use by FTAM".

[18] ISO/IEC ISP 10607-2 (1995): "Information technology - International Standardized Profiles AFTnn - File Transfer, Access and Management - Part 2: Definition of Document Types, Constraint sets and Syntaxes".

[19] ISO/IEC ISP 10607-3 (1995): "Information technology - International Standardized Profiles AFTnn - File Transfer, Access and Management - Part 3: AFT 11 - Simple File Transfer Service (Unstructured)".

[20] Void

[21] Void

[22] ITU-T Recommendation X.25 (1996): "Interface between Data Terminal Equipment (DTE) and Data Circuit Terminating Equipment (DCE) for Terminals operating in the Packet Mode and connected to Public Data Networks by Dedicated Circuit".

[23] ... [42] Void

[43] ISO/IEC 7776 (1995): "Information technology - Telecommunications and information exchange between systems - High-level data link control procedures - Description of the X.25 LAPB-compatible DTE data link procedures".

[44] ISO/IEC 8208 (2000): "Information technology - Data communications - X.25 Packet Layer Protocol for Data Terminal Equipment".

[45] ISO/IEC 8878 (1992): "Information technology - Telecommunications and information exchange between systems - Use of X.25 to provide the OSI Connection-mode Network Service".

[46] IETF RFC 1006: "ISO Transport on top of the TCP", Marshall T. Rose, Dwight E. Cass, Northrop Research and Technology Center, May 1987. Status: Standard.

[47] IETF RFC 793: "Transmission Control Protocol (TCP)", September 1981. Status: Standard.

[48] IETF RFC 791: "Internet Protocol (IP)", September 1981. Status: Standard.

[49] ITU-T Recommendation X.680 (2002): "Information Technology-Abstract Syntax Notation One (ASN.1): Specification of Basic Notation".

[50] 3GPP TR 21.905: "Vocabulary for 3GPP Specifications".

[51] 3GPP TS 22.115: "Service aspects; Charging and Billing".

[52] The Object Management Group (OMG) "The Common Object Request Broker: Architecture and Specification", Revision 2.1, August 1997. http://www.omg.org/technology/documents/vault.htm#CORBA_IIOP

[53] 3GPP TS 32.400-series: "Telecommunication management; Performance Management (PM)".

[54] 3GPP TS 32.600: "Telecommunication management; Configuration Management (CM); Concept and high-level requirements".

[55] 3GPP TS 32.240: "Telecommunication management; Charging management; Charging architecture and principles".

[56] 3GPP TR 22.121: "Service aspects; The Virtual Home Environment; Stage 1".

[57] 3GPP TS 32.140: "Telecommunication management; Subscription Management (SuM) requirements".

[58] 3GPP TS 32.141: "Telecommunication management; Subscription Management (SuM) architecture".

[59 to 99] Void

[100] TMF GB910: "Telecom Operations Map"; Approved Version 2.1 March 2000, (may be downloaded from http://www.tmforum.org.).

[101] 3GPP TS 32.102: "Telecommunication management; Architecture".

[102] ITU-T Recommendation M.3013 (2000): "Considerations for a telecommunications management network".

[103] Void.

[104] 3GPP TR 21.801: "Specification Drafting Rules".

[105] TMF GB910B: "Telecom Operations Map Application Note-Mobile Services: Performance Management and Mobile Network Fraud and Roaming Agreement Management"; Public Evaluation Version 1.1, September 2000. (May be downloaded free from http://www.tmforum.org.)

[106] OMA Service Provider Environment Requirements, OMA-RD-OSPE-V1_0-20050614-C, The Open Mobile Alliance™ (URL:http://www.openmobilealliance.org/).

[107] 3GPP TR 32.806: "Telecommunication management; Application guide for use of Integration Reference Points (IRPs) on peer-to-peer (p2p) interface".

[108] W3C SOAP Version 1.1 recommendation (http://www.w3.org/TR/2000/NOTE-SOAP-20000508/).

[109] W3C SOAP Version 1.2 recommendation (http://www.w3.org/TR/soap12-part1/).

[110] 3GPP TR 32.809: "Telecommunication management; Feasibility study of XML-based (SOAP/HTTP) IRP solution sets".

[111] 3GPP TS 32.150: V7.0.0"Telecommunication management; Integration Reference Point (IRP) Concept and definitions".

[112] ITU-T Recommendation M.3050.x (2006) series Enhanced Telecom Operations Map (eTOM).

[113] ITU-T Recommendation M.3050.1 (2004) Enhanced Telecom Operations Map (eTOM) – The business process framework.

[114] ITU-T Recommendation M.3050.2 (2004) Enhanced Telecom Operations Map (eTOM) – Process decompositions and descriptions.

[115] TR-069 Amendment 2, CPE WAN Management Protocol v1.1, Broadband Forum

[116] WS-I Basic Profile 1.1; http://www.ws-i.org/Profiles/BasicProfile-1.1.html

[117] W3C Web Services Description Language (WSDL) 1.1; http://www.w3.org/TR/wsdl

[118] IETF RFC 6241 Network Configuration Protocol (NETCONF); June 2011.

[119] 3GPP TS 32.107: “Fixed Mobile Convergence (FMC) Federated Network Information Model (FNIM)”.

3 Definitions and abbreviations

3.1 Definitions

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

Domain Manager (DM): provides element management functions and domain management functions for a sub-network. Inter-working domain managers provide multi vendor and multi technology network management functions.

Element Manager (EM): provides a package of end-user functions for management of a set of closely related types of network elements. These functions can be divided into two main categories: Element Management Functions and Sub-Network Management Functions.

Element Management functions: for management of network elements on an individual basis. These are basically the same functions as supported by the corresponding local terminals.

Enterprise Systems: Information Systems that are used in the telecommunication organisation but are not directly or essentially related to the telecommunications aspects (Call Centre's, Fraud Detection and Prevention Systems, Invoicing etc).

Information Service (IS): Defined in 3GPP TS 32.150 [111].

Integration Reference Point (IRP): Defined in 3GPP TS 32.150 [111].

Managed Object: Defined in 3GPP TS 32.150 [111].

Management Infrastructure: the collection of systems (computers and telecommunications) a PLMN Organisation has in order to manage its network.

Network Element (NE): a discrete telecommunications entity, which can be managed over a specific interface, e.g. the RNC.

Network Manager (NM): provides a package of end-user functions with the responsibility for the management of a network, mainly as supported by the EM(s) but it may also involve direct access to the Network Elements. All communication with the network is based on open and well-standardized interfaces supporting management of multi-vendor and multi-technology Network Elements.

NML Service (NMLS): It is a NM layer logical entity which is separated from the functionality of the NM. The NMLS is a generic representation of a certain kind of function which has a standardized interface to the NM. The specific functionality on the interface depends on the kind of function.

Network Resource Model (NRM): Defined in 3GPP TS 32.150 [111].

Operations System (OS): a generic management system, independent of its location level within the management hierarchy.

Public Land Mobile Network (PLMN): see 3GPP TR 21.905 [50].

PLMN Organisation: legal entity that is involved in the management of a telecommunications network providing mobile cellular services.

Service: see 3GPP TR 21.905 [50].

Service Level Tracing: see OMA Service Provider Environment Requirements, OMA-RD-OSPE-V1_0-20050614-C [106].

Solution Set (SS): Defined in 3GPP TS 32.150 [111].

Sub-Network management functions: functions related to a network model for a set of Network Elements constituting a clearly defined sub-network, which may include relations between the Network Elements. This model enables additional functions on the sub-network level (typically in the areas of network topology presentation, alarm correlation, service impact analysis and circuit provisioning).

3.2 Abbreviations

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

API	Application Programming Interface
ASN.1	Abstract Syntax Notation One
ATM	Asynchronous Transfer Mode
B2B	Business to Business
B-ISDN	Broadband ISDN
BBF	Broadband Forum
BOOTP	Boot protocol
CLI	Command Line Interface
COPS	Common Open Policy Service
COPS-PR	COPS Usage for Policy Provisioning
CORBA IIOP	Common Object Request Broker Architecture Internet Inter-ORB Protocol
CORBA	Common Object Request Broker Architecture
CORBA/IDL	Common Object Request Broker Architecture/Interface Definition Language
DCN	Data Communications Network
DECT	Digital Enhanced Cordless Telecommunications
DHCP	Dynamic Host Configuration Protocol
DM	Domain Manager
DNS	Directory Name Service
DSS1	Digital Subscriber System 1
EM	Element Manager
EML	Element Manager Layer
EMS	Element Management System
ES	Enterprise Systems
eTOM	Enhanced Telecom Operations Map® (TeleManagement Forum)
FFS	For Further Study
FMC	Fixed Mobile Convergence
FNIM	Federated Network Information Model
FTAM	File Transfer Access and Management
FTP	File Transfer Protocol
ftp	FTP
GGSN	Gateway GPRS Support Node
Go interface	The interface between the GGSN and the Policy Decision Function (PDF)
GSM	Global System for Mobile communications
HLR	Home Location Register
HSS	Home Subscriber Server
IDL	Interface Definition Language
IETF	Internet Engineering Task Force
IIOP	Internet Inter-ORB Protocol
IN	Intelligent Network
INAP	Intelligent Network Application Part
IRP	Integration Reference Point
IS	Information Service
ISDN	Integrated Services Digital Network
LDAP	Lightweight Directory Access Protocol
LDUP	LDAP Duplication/Replication/Update Protocols
LLA	Logical Layered Architecture

LSA	Licensed Shared Access
MAP	Mobile Application Part
MExE	Mobile Execution Environment
MIB	Management Information Base
MMI	Man-Machine Interface
NE	Network Element
NM	Network Manager
NML	Network Management Layer
NMLS	Network Management Layer Service
NMS	Network Management System
NRM	Network Resource Model
OAM&P	Operations, Administration, Maintenance and Provisioning
OS	Operations System
OSI	Open Systems Interconnection
OSS	Operations Support System
p2p	Peer-to-Peer
PDF	Policy Decision Function
PDH	Plesiochronous Digital Hierarchy
PDP	Policy Decision Point
PIB	Policy Information Base
PKI	Public Key Infrastructure
PLMN	Public Land Mobile Network
PSTN	Public Switched Telephone Network
QoS	Quality of Service
QoE	Quality of Experience
QMC	QoE Measurement Collection
RNC	Radio Network Controller
RSVP	Resource ReserVation Protocol
SAP	Service Access Point
SC	Service Consumer
SD	Service Directory
SDH	Synchronous Digital Hierarchy
sftp	secure ftp
SLA	Service Level Agreement
SNMP	Simple Network Management Protocol (IETF)
SNMP/SMI	SNMP/Structure of Management Information
SOA	Service Oriented Architecture
SOM	Service Operations Management
SP	Service Provider
SS	Solution Set
SS7	Signalling System No. 7
SSH	Secure Shell
SSL	Secure Sockets Layer
TCP/IP	Transmission Control Protocol/ Internet Protocol
tftp	trivial ftp
TM	Telecom Management
TMF	TeleManagement Forum
TMN	Telecommunications Management Network (ITU-T)
TOM	Telecom Operations Map (TMF)
UE	User Equipment
UIM	Umbrella Information Model
UML	Unified Modelling Language
UPT	Universal Personal Telecommunication
USIM	Universal Subscriber Identity Module
UTRA	Universal Terrestrial Radio Access
VHE	Virtual Home Environment
WSDL	Web Service Description Language (W3C)

4 General

4.1 PLMN Telecom Management

4.1.1 Basic objectives for PLMN management

The following basic objectives to be supported by the management specifications have been identified:

- to be capable of managing equipment supplied by different vendors including the management systems themselves.
- to minimise the complexity of PLMN management.
- to provide the communication between Network Elements (NEs) and Operations Systems (OS) or between OSs themselves via standardised interfaces (e.g. CORBA, SNMP, etc.) as appropriate and necessary.
- to minimise the costs of managing a PLMN such that it is a small component of the overall operating cost.
- to provide configuration capabilities that are flexible enough to allow rapid deployment of services.
- to provide integrated Fault Management capabilities.
- to simplify maintenance interventions by supporting remote maintenance operations.
- to allow interoperability between Network Operators/Service Providers for the exchange of management/charging information. This includes interoperability with other networks and services (e.g. ISDN/B-ISDN, PSTN and UPT) as well as other PLMNs.
- to enable the support and control of a growing number of resources. This would allow the system to start from a small and simple configuration and grow as needed, both in size and complexity.
- to re-use existing relevant standards (e.g. GSM, IN, ISDN/B-ISDN, ITU-T, TMF etc.) where applicable.
- to support the security management of PLMNs (e.g. key management, access control management, operation and administration of security mechanisms) with particular emphasis on new features such as automatic roaming and packet switched services.
- to provide and support a flexible billing and accounting administration, to support charging across PLMNs.
- to address the management and assessment of system performance and operation through the use of common measurements, etc. This would enable a Network Operator/Service Provider to assess actual performance against planned targets.
- to expose any information only once.
  (Example: In case an operator would like to change one parameter in a cell: Then all occurrences of this parameter, e.g. transceiver frequency, hand-over relationships, performance measurements, frequency hopping control, etc., should be changed by one action only.)
- to support the restoration of an Operations System (e.g. resynchronisation and atomic transactions).
- to have one (1) name convention for network resources under management in the 3GPP context. To perform network management tasks, co-operating applications require identical interpretation of names assigned to network resources under management. Such names are required to be unambiguous as well.

It is acknowledged that the introduction of new architecture to support new services or the introduction of new services themselves may impact the detailed requirements of some or all of the above.

4.1.2 3GPP reference model

A 3GPP System is made of the following components:

- one or more Access Networks, using different types of access techniques (GSM, UTRA, DECT, PSTN, ISDN, ...) of which at least one is UTRA;
- one or more Core Networks;
- one or more Intelligent Node Networks service logic and mobility management, (IN, GSM ...);
- one or more transmission networks (PDH, SDH etc.) in various topologies (point-to-point, ring, and point-to-multi-point...) and physical means (radio, fibre and copper ...).

The 3GPP system components have signalling mechanisms among them (DSS1, INAP, MAP, SS7, RSVP,...).

From the service perspective, the 3GPP system is defined to offer:

- Service support transparent to the location, access technique and core network, within the bearer capabilities available in one particular case;
- User to terminal and user to network interface (MMI) irrespective of the entities supporting the services required (VHE);
- Multimedia capabilities.

4.1.3 3GPP provisioning entities

TS 22.101 "Services Principles" [2] identifies two major entities, which cover the set of 3GPP functionalities involved in the provision of the 3GPP services to the user. These are:

Home Environment: This entity holds the functionalities that enable a user to obtain 3GPP services in a consistent manner regardless of the user's location or the terminal used;

Serving Network: This entity provides the user with access to the services of the Home Environment.

4.1.4 Management infrastructure of the PLMN

Every PLMN Organisation has its own management infrastructure. Each management infrastructure contains different functionality depending on the role-played and the equipment used by that PLMN Entity.

However, the core management architecture of the PLMN Organisation is very similar. Every PLMN Organisation:

- provides services to its customers;
- needs an infrastructure to fulfil them (advertise, ordering, creation, provisioning ...);
- assures them (Operation, Quality of Service, Trouble Reporting and Fixing ...);
- bills them (Rating, Discounting ...).

Not every PLMN Organisation will implement the complete management architecture and related processes. Some processes may be missing dependent on the role a particular organisation is embodying. Processes not implemented by a particular organisation are accessed via interconnections to other organisations, which have implemented these processes (called X-interfaces in the ITU-T TMN architecture).

The management architecture itself does not distinguish between external and internal interfaces.

4.2 ITU-T TMN

ITU-T TMN (Telecommunications Management Network standard from the ITU-T), as defined in ITU-T Recommendation M.3010 [1], provides:

- an architecture, made of OS (Operations Systems) and NEs (Network Elements), and the interfaces between them (Q, within one Operator Domain and X, between different Operators);
- the methodology to define those interfaces;
- other architectural tools such as LLA (Logical Layered Architecture) that help to further refine and define the management architecture of a given management area;
- a number of generic and/or common management functions to be specialised/applied to various and specific ITU-T TMN interfaces.

The PLMN Management Architecture is based on ITU-T TMN, and will reuse those functions, methods and interfaces already defined (or being defined) that are suitable to the management needs of a PLMN.

Another management approach that is employed is the Telecom Operations Map from TeleManagement Forum (TMF). The Telecom Operations Map, using the TMN model as a foundation, addresses operation support and management for any communications service from a top down customer oriented standpoint.

5 Architectural framework

5.1 Management reference model and interfaces

5.1.1 Overview

Figure 1 illustrates the management reference model. It shows the Operations Systems interfacing with other systems.

The present document (and the rest of the 3GPP management detailed specifications) addresses the Operations System (function and architecture wise) and the interfaces to the other systems (information and protocol wise).

The present document does not address the definition of any of the systems, which the Operations System may interface to. The rest of the 3GPP specifications regarding management will not cover them either.

It is not the approach (nor it is possible) to re-define the complete management of all the technologies that might be used in the provision of a PLMN. However, it is the intention to identify and define what will be needed from the perspective of management.

An Operations System supports management interfaces to other systems. In each Operations System, a number of functions are present. The function(s) in execution would effectuate how the Operations System would interface to other systems.

Examples of functions and entities included at the Network Management layer in an Operations System may include but are not limited to:

- Management and Orchestration, of network services.
- On-line network support for 3GPP services.
- Network planning including Radio Planning.
- Network Configuration Management.
- SON automation Management and Orchestration.
- Alarm correlation.
- Network event correlation.
- Network Supervision.
- Network Performance Monitoring.
- Operator terminal.
- LSA Controller (LC).
- IRP Manager.

Examples of functions and entities included at the Domain/Element Management layer in an Operations System may include but are not limited to:

- Network Configuration Management.
- Alarm correlation.
- Network Performance Monitoring.
- SON automation Management and Orchestration.
- Operator terminal.
- IRP Agent.

A number of management interfaces in a PLMN are identified in figure 1, namely:

1) between the Network Elements (NEs) and the Element Manager (EM) of a single PLMN Organisation;

2) between the Element Manager (EM) and the Network Manager (NM) of a single PLMN Organisation;

NOTE: In certain cases the Element Manager functionality may reside in the NE in which case this interface is directly from NE to Network Manager). These management interfaces are given the reference name Itf-N and are the primary target for standardization.

3) between the Network Managers and the Enterprise Systems of a single PLMN Organisation;

4) between the Network Managers (NMs) of a single PLMN Organisation;

4a) between the Domain Managers (DMs) of a single PLMN Organisation.

5) between Enterprise Systems & Network Managers of different PLMN Organisations;

5a) between the Domain Managers (DMs) of different PLMN Organisations.

6) between Network Elements (NEs).

7) between the Network Management Layer Service (NMLS) and the Network Manager (NM).

IRPs may be implemented at interfaces 2, 3, 4, 5 and 7.

The present document identifies Type 1, Type 2 and Type 4 management interfaces. The rest of the 3GPP management specifications focus on Type 2 and to a lesser extent on Type 1 management interfaces. In addition, the rest of the 3GPP management specifications will not refer to Type 4 management interface. Specific Type 2 protocols and information model that are applicable for use in Type 4 management interface are listed in Annex E.

The present document identifies Types 3, 5 & 5a management interfaces. Detailed specification of these interfaces is For Further Study (FFS).

The present document identifies as well a Type 7 management interface.

The specification of the management interfaces of type 4 & 6 is beyond the scope of standardisation.

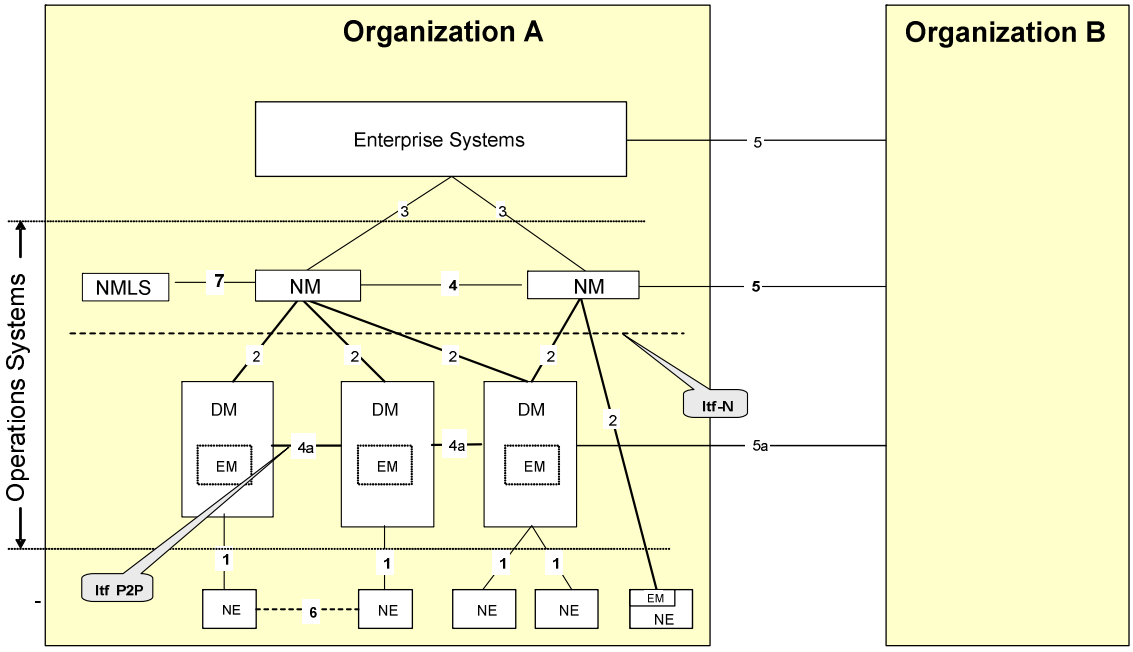


Figure 1: Management reference model

5.1.2 Interfaces from Operations Systems to NEs (Type 1 & 2)

In some cases, the management interfaces to NEs have been defined bottom-up, trying to standardise the complete OAM&P functionality of the various NEs.

For PLMN management, a top-down approach will be followed to streamline the requirements from the perspective of Operators top priority management processes.

It is assumed that this will not fully cover the OAM&P functionality of all NE types at once; therefore a part of the functionality will be phased for further work and consideration. Some proprietary solutions (local and/or remote) will be needed in the interim. The rationale of this approach is not only the best use of resources, but also to follow a pragmatic step-wise approach that takes into account the market forces (the manufacturers and operators capabilities). A further rationale is to define clear and easy-to-agree steps that allow management functionality to be implemented in the same time frame as the telecom functionality in the network (i.e. to synchronise the management and network releases).

5.1.2.1 Interfaces from EM Operations Systems to NEs (Type 1)

The approach for NE management interfaces of Type 1 will be to allow the use of certain management application layer protocols (Management-application-layer-protocols). See Annex A for the list of Management-application-layer-protocols.

5.1.2.2 Interfaces from NM Operations Systems to NEs (Type 2)

The approach for NE management interfaces of Type 2 will be to concentrate on Management-application-layer-protocol independent information models (see 5.2.2 Information Model Level), allowing a mapping to several Management-application-layer-protocols (see 5.2.3 Solution Set Level). The rational is:

- Due to the convergence of Information and Telecommunication technologies, it is required to work on a more open approach (acknowledging the market status and foreseen evolutions);
- The life cycle of information flows, characterised by information models, is 10 to 20 years, while that of Management-application-layer-protocols is 5 to 10 years;
- Developments in automatic conversion from information models to various Management-application-layer-protocols will allow a more pragmatic and open approach (e.g. UML to IDL).

However, it is the intention to at least recommend one mapping for each information model defined.

Figure 2 shows the management interfaces of one part of the 3GPP System (the Radio Network), by way of illustration of interfaces of types 1 and 2.

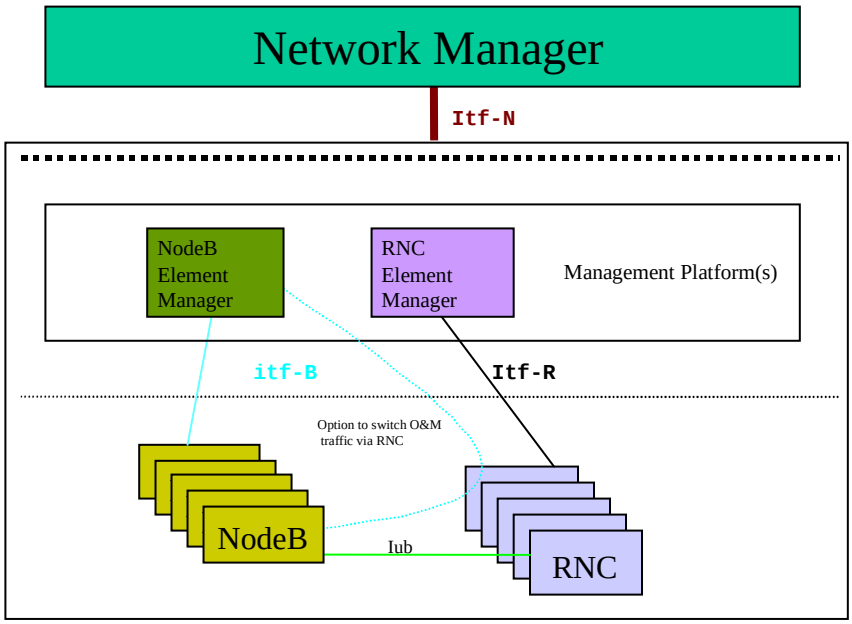


Figure 2: Radio Network management interfaces

Figure 2 identifies the following management interfaces:

- Itf-B - between Node B & its Manager (physically, this may be a direct connection or via the RNC) (type 1).
- Itf-R - between RNC & its Manager (type 1).
- Itf-N – between the Network (Element Manager or NEs with an embedded EM) & Network Manager (type 2).

5.1.3 Interfaces to Enterprise Systems (Type 3)

The approach is to define a management structure that fully fits into the enterprise process needs of the PLMN Organisations. One of the essential issues of today's way of running telecommunications businesses is integral operation (e.g. customer care, from service subscription to billing, from order fulfilment to complaint management).

Enterprise Systems are those Information Systems that are used in the telecommunication organisation but are not directly or essentially related to the telecommunications aspects (Call Centres, Fraud Detection and Prevention Systems, Invoicing etc.).

Standardising Enterprise Systems is out of the scope of 3GPP work, since it involves many operator choices (organisational, etc.) and even regulatory. Also Enterprise Systems are often viewed as a competitive tool. However, it is essential that the requirements of such systems are taken into account and interfaces to the Operations Systems are defined, to allow for easy interconnection and functional support.

5.1.3a Interface between Network Managers (Type 4)

Interface type 4 (where Itf-P2P is between Domain Managers of different PLMN Organisations) could have additional requirements over interface type 4a (see clause 5.1.3b) and therefore is FFS.

5.1.3b Interface between Domain Managers (Type 4a) - the Itf-P2P Interface

The approach for Interfaces of type 4a (the Itf-P2P interface) is the same as for interfaces of type 2 (the Itf-N interface – see clause 5.1.2.2).

The Itf-P2P should as much as possible re-use the interface definitions of the Itf-N interface.

Further details on the Itf-P2P interface are available in 3GPP TR 32.806 [107].

5.1.4 Interfaces to Operations Systems in other organisations (Type 5)

PLMN management considers integrally the interaction with the Operations Systems of other legal entities for the purpose of providing Mobile services.

There are two major types of interfaces to other management systems:

1) To the Operations Systems of another PLMN Organisation;

2) To the Operations Systems of a non-PLMN Organisation.

The first type deals with co-operation to provide Mobile services across a number of PLMN networks (e.g. roaming related interactions). The second type deals with client-server relationship to other operators (e.g. to leased lines providers, to added value service providers, etc.).

The approach that will be followed is to identify and define integral processes, not taking into account in the first step, how many operators or operations systems might be involved, but rather concentrating on the interactions between them (i.e. assuming an operator encompasses all functionalities). A further step will be to consider and define extra requirements (security, confidentiality etc.) when part of the process involves interactions with other operators Operations Systems (OSs).

5.1.5 Inter-NE interfaces (Type 6)

Interfaces between Network Elements are sometimes used to carry management information even though this may not be the primary purpose of the interface. An example in an UMTS network is the I_{ub} interface between Node-B and RNC (see figure 2 above). This type of interface is not within the scope of this specification, though potential impacts upon it should be considered.

5.1.6 Interface between NMLS and NM (Type 7)

The Type 7 interface is between the NMLS and the NM. The NMLS is the Service Provider (SP, see clause 5.4) and the NM the Service Consumer (SC, see clause 5.4).

5.2 Interface levels

5.2.1 Overview

The management interfaces are studied here from five different perspectives or levels:

1) Information Model Level (network resource model and interactions used between manager and agent, or equivalent);
2) Solution Set (SS) Level;
3) Application protocol (end-to-end, upper layers protocol running between manager-agent, or equivalent);
4) Networking protocol (lower layer protocols carrying the information in/out the manager and agent, or equivalents);
5) Physical (mapping of the manager and agent, or equivalents, roles into physical entities).

5.2.2 Information Model level

This level defines the network resources under management and the management information exchanged between manager-agent, and equivalent, across the management interface.

Type 2 and type 4a interfaces (Itf-N and Itf-P2P in figure 1) require the specification at this level and at the level defined in 5.2.3.

5.2.3 Solution Set (SS) level

For an NRM or an Interface at the Information Model, there will be at least one Solution Set defined. A Solution Set is a mapping of the Information Model to one of several Management-application-layer-protocols.

See annex C for the valid 3GPP management IRP Solution Sets (see also ITU-T Recommendation M.3013-2000 [102]).

5.2.4 Management-application-layer-protocol level

This level covers the set of primitives used to pass information across a given interface and the means to establish associations between the application entities (including the related addressing aspects) across a given interface.

3GPP recommends a set of Management-application-layer-protocols (see Annex A).

5.2.5 Networking protocol level

Whatever standardised protocol suite at the networking level that is capable of meeting the functional and operational requirements (including the network addressing aspects) of the Logical and Application Protocol levels of a given management interface, is a valid Networking Protocol for that interface.

A number of requirements shall be met by the Networking Protocol, as follows:

- capability to run over all supported bearers (leased lines, X.25, ATM, Frame Relay ...);
- support of existing transport protocols and their applications, such as OSI, TCP/IP family, etc.;
- widely available, cheap and reliable.

The Internet Protocol (IP) is a Networking Protocol that ideally supports these requirements. IP also adds flexibility to how management connectivity is achieved when networks are rolled out, by offering various implementation choices. For instance, these may take the form of:

- Dedicated management intranets.
- Separation from or integration into an operator's enterprise network.
- Utilisation, in one-way or another, of capacities of the public Internet and its applications or other resources.

5.2.6 Physical level

Though the interaction at the logical level takes place between the management system and the NEs, it is left to the implementer's choice the possibility to use the Q-Adapter concept of ITU-T TMN Architecture as physical implementation (as defined in ITU-T Recommendation M.3010 [1]).

The present document does not preclude the usage of Q-Adapters at other PLMN management interfaces.

5.3 3GPP compliance conditions

For a 3GPP entity (management system or NE) to be compliant to a given management interface, all the following conditions shall be satisfied:

- it implements the management functionality following the Information Service specified by the relevant 3GPP management interface specifications applicable to that interface;
- it provides at least one of the IRP Solution Sets (see Annex C) related to the valid application protocols specified by 3GPP application protocols for that interface (see annex A). For each interface at least one of the valid protocols will be recommended;
- it provides at least one standard networking protocol (see Annex B);
- in case the entity does not offer the management interface on its own, a Q-Adapter shall be provided. This Q adapter shall be provided independently of any other NE and/or management system.

5.4 Service Oriented Architecture (SOA)

5.4.1 Basic elements of SOA

The basic building block of SOA is a *service*. In the context of this document, the word service is used to denote the various kinds of network management services, provided or provisioned by and consumed by network management applications. This type of network management services are distinct from those that are consumed by, say, mobile phone subscribers. One example of this type of network management service is one that is used for the management of alarm information of a network. Another example can be one that is used for the management of the transfer of large amount of network management information in files.

A service, in the context of this document, is considered a black box whose internal design and characteristics are of no relevance. A service performs tasks that satisfy a specific set of requirements. A service is realized by a Service Provider (SP) entity. This entity, the SP, is responsible to register (re: using the registerService offered by SD to SP of the following diagram) its provisioned service in one or more Service Directory (SD) entities. Service Consumers (SCs), without prior knowledge of the kind of services provisioned and the service access point (SAP) of the provisioned service, can consult the SD for the information (re: using the locateService offered by SD to SC of the following diagram). Once the SC discovers the wanted provisioned service and its associated SAP, it can contact the SP and start consuming the wanted provisioned service (re: using the useService offered by SP to SC of the following diagram).

Using the basic interaction scenario described above, a new SC can be installed and activated without prior knowledge of its wanted service SAP(s). As long as a) the new SC is given the SAP of the SD and b) the SP providing the wanted service has registered its service with the SD, the new SC can discover the availability of its wanted service and its SAP, and thus, can begin to access the service wanted.

Similarly, a new SP can be installed and activated (i.e. to provision its service) without prior knowledge of its potential SC(s). It is required to register its provisioned service with SD(s).

The SD is a special kind of SP. It provides two kinds of services. One service supports the registration of the identity, availability and SAP of the provisioned service (re: registerService offered by SD to SP of the following diagram). The other service supports the discovery of services (re: locateService offered by SD to SC of the following diagram).

The SDs' SAPs for providing registration of provisioned service should be made known to all SPs. The SDs' SAPs for discovery of provisioned service should be made known to all SCs. The means by which these SAPs are make known to SCs and SPs are not subject to standardization.

The NE, EM, NM and DM of Figure 1 are entities that contain a SP. The DM, NM and Enterprise System of Figure 1 are entities that contain a SC.

The following diagram depicts the key elements of SOA and their relations. The relation is depicted by an arrow with a label. The arrow end indicates the consumer of the network management service. The other end indicates the provider of the service. The label identifies the service.

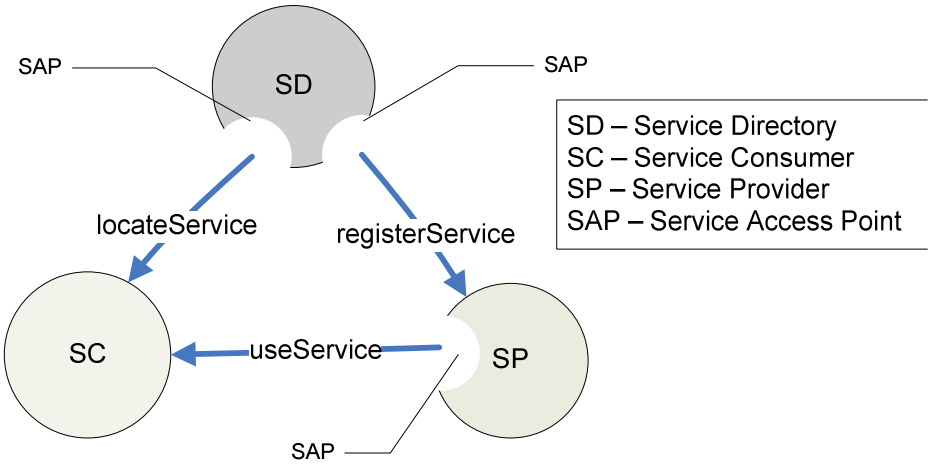


Figure 2a: SOA basic elements

5.4.2 Aggregation of SOA basic elements

An entity can have one or more SCs and SPs at the same time. This entity can consume services from SPs, add its own value using internal function such as service aggregation, correlation, service request redirection, information store and forward service, etc (re F of the following diagram), and provide a new set of enhanced service to other potential SCs. To play the role of SP, this entity would need to register its enhanced service with SD. The diagram below depicts such entity.

The DM and NM of Figure 1 are of this entity kind.

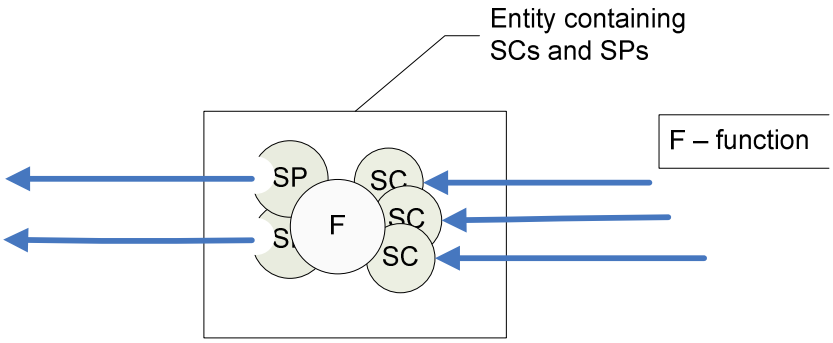


Figure 1b: Entity produces and consumes services

5.4.3 Information transfer bus

SPs, SCs and SDs transfer information among themselves. For example, a SC would send a service request to a SP. In SOA, a bus-like concept is used to depict the capability of such information transfer. This bus-like concept support a key attribute of SOA in that its basic elements, namely SP, SC and SDs, are all loosely-coupled, e.g. their bindings are to be established on need and at run-time basis.

The following figure depicts the loosely-coupled SOA elements supported by the Information transfer bus.

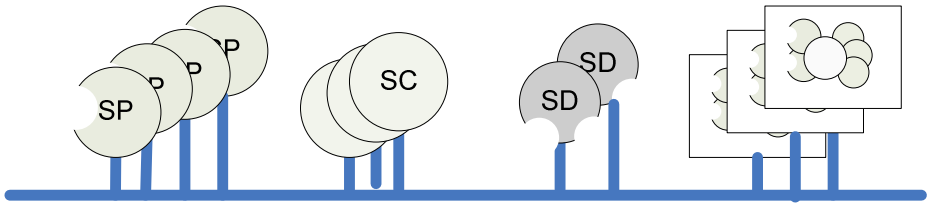


Figure 2c: Information transfer bus supporting SOA elements

5.4.4 SOA elements within the Management reference model

This clause shows the placement of SOA basic elements SPs and SCs within the Management reference model (see Figure 1).

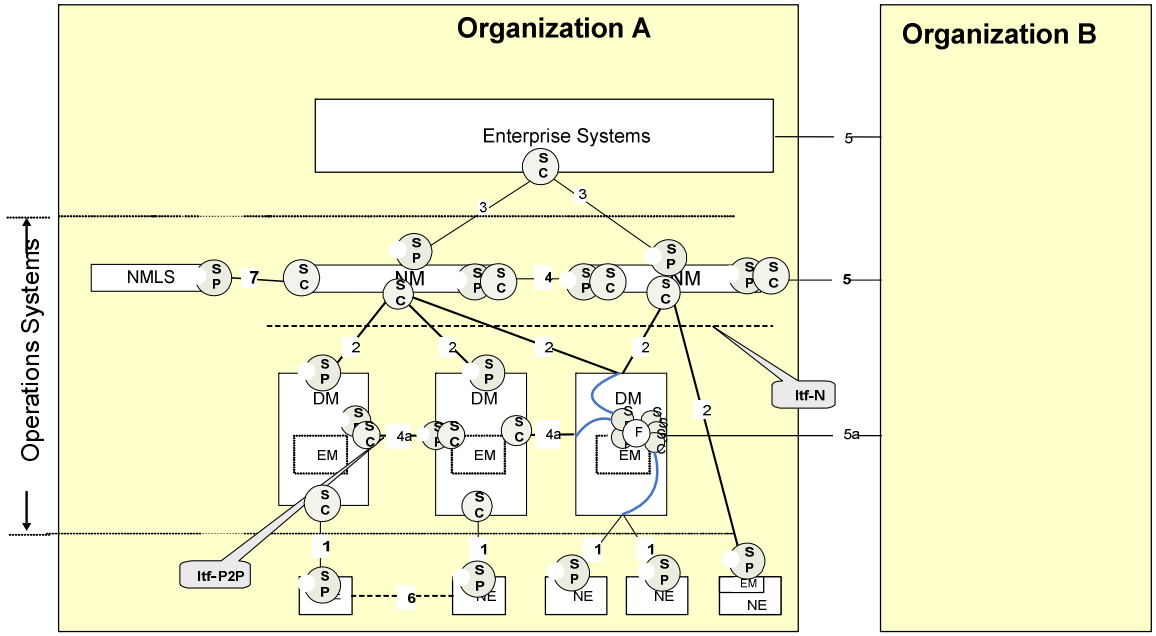


Figure 2d: Placement of SOA elements on Management reference model

For example, the right-hand side DM (a Management reference model construct) of Figure 2d shows an entity that is an aggregation of SOA basic elements (see clause 5.4.2). This entity produces and consumes services (see Figure of clause 5.4.2). It has two SPs and three SCs. In addition, it has an F function that mediates between services DM provides and the services DM requires. The DM services are provided to one SC of the neighboring DM and to two SCs of two NMs. The DM requires services from two SPs of the two NEs. One of the SPs of this DM provides a network management service via the Type 2 interface. One of the SPs supports the peer-to-peer protocol by offering services to its neighboring DM via Interface 4a. Three SCs of this DM are consumer of network management services offered by two NEs via the Type 1 interface.

To avoid cluttering the figure, SDs are not shown in Figure 2d. Conceptually, SDs can be positioned anywhere in the Management reference model. For example, the most likely configuration is to have SDs placed within the Operations Systems boundary. They can either be embedded inside NM and/or DM and/or stand-alone. Note that an SD embedded, say in DM-1, does not imply that this particular SD would/could only register services provided by DM-1. To avoid cluttering the figure, F function is only shown in one DM but all DMs and NMs can have F function as well.

The question if the protocols supporting the locateService and registerService (see Figure 2a) are of Type 1 or Type 2 or Type 4, etc can only be answered if the placement of SD and its clients (i.e. SC and SP) in the Management reference model are known.

5.4.5 SOA-based representation of the Management Reference Model

This section provides another SOA-based view of the 3GPP Management Reference Model that includes the paths where network management information would flow (SOA data path). This view is derived from and in accordance with Figure 4: “Placement of SOA elements on Management reference model”.

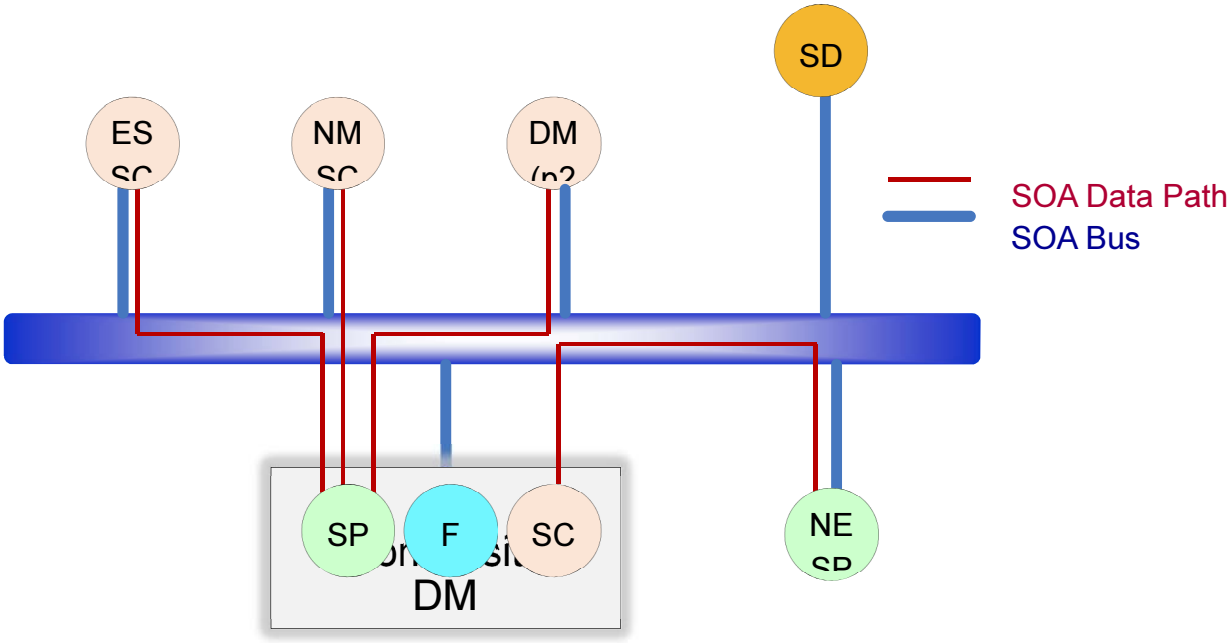


Figure 5: SOA-based representation of the 3GPP Management Reference Model

Figure 5 depicts the communication over the SOA bus. Serving management entities (i.e. SP) are connected to the SOA bus with functionality exposed as a service. SPs can be registered and discovered via the SD, and they can also be composite services that connect to or reuse other SPs (i.e Composite DM). Consuming management entities (i.e. SC) are also connected to the SOA bus and can discover available services via the SD, and subsequently use services of SPs.

5.4.6 SOA-supporting Solution Set

SOA-supporting Solution Set definitions can be found in Annex C.

5.5 Converged Management

5.5.1 Introduction to FNIM

On-going industry convergence and pressure to reduce cost is placing an ever-increasing emphasis on the need to rationalize and align various network management aspects across boundaries of standards/specifications producing organizations. The cost, resulting from integration and management challenges, of the lack of a coherent treatment of the whole network has becoming increasingly apparent to the point where operators of networks are demanding action.

The Federated Network Information Model [119] is covering all key aspects of a solution to the on-going industry convergence challenge. It focuses on Information Model federation and is constructed to best deal with the various contradictory pressures of the current environment providing a pragmatic and realizable approach.

5.5.2 FNIM Features

The following FNIM features are essential for the maintenance of the integrity of a large and scalable FMC network model:

- An FMC network model that is partitioned into model components.
- Defines an Umbrella Information Model (UIM) that is further partitioned to allow broad industry participation.
- Enables navigation among instances of different model components.
- Has the ability to import model elements designed elsewhere.

- Provides independence of tools and platforms.
- Is independent of solution technologies and access protocol designs.
- Utilizes industry experience.
- Supports release handling per model components.

5.5.3 FNIM Elements

5.5.3.1 FNIM components

The Umbrella Information Model (UIM) provides abstract definitions applicable across Domain/Technology-specific Concrete Models to enable end-to-end consistency of such definitions (it is described as 'abstract' in the sense that its components are used via "special linkages" by Domain/Technology-specific Concrete Models, and that it is not designed for the purpose of partial or full instantiation of its components and is not sufficient to provide meaningful network management service).

Domain/Technology-specific Concrete Models are described as 'concrete models' in the sense that their instantiation is necessary to provide meaningful management services. These Domain/Technology-specific Concrete Models uses "special linkages" with the common definitions of the Umbrella Information Model (UIM) for the purpose of end-to-end consistency of management information semantics. In addition, these Domain/Technology-specific Concrete Models have specified relationships between each other to enable end-to-end monitoring and management of a converged network.

5.5.3.2 Relations between model components (including UIM)

This section provides a graphical representation of the FNIM in terms of relation between model components.

There are two areas considered:

- The definitions of the classes inside the UIM model component.
- The definitions of relation (R0 in Figure 5.5.3.2-1) used between various classes in UIM model component and other model components.

The aim is to have identical R0 for use between the UIM model component and other model components while the UIM model component need to have no knowledge of its usage by classes of other model components. This will ensure consistency (e.g. resource management style, paradigm) for managing mobile managed resources, as well as other managed resources such as transport managed resources.

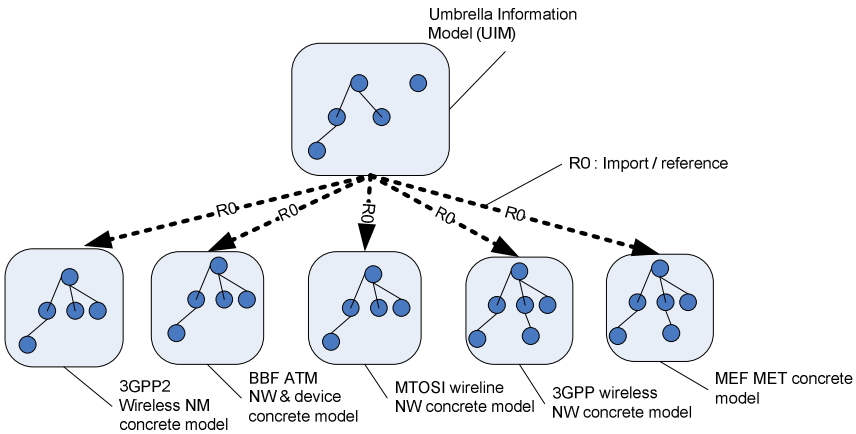


Figure 5.5.3.2-1: Relation between UIM model component and other model components

Taking the example of "3GPP wireless network classes" and the UIM, 3GPP model components would import relevant UIM classes and make derivatives for their use. R0 in this case is an inheritance relation. There are other forms of relations that could be defined.

5.5.3.3 Relations among pairs of model components

This section provides a graphical representation of the FNIM in terms of bilateral relation between each pair of model components, neither of which is a UIM model component.

The relation between pairs of model components may not be same. Each relation may or may not be symmetrical. UIM may not be involved in such pair-wise relations.

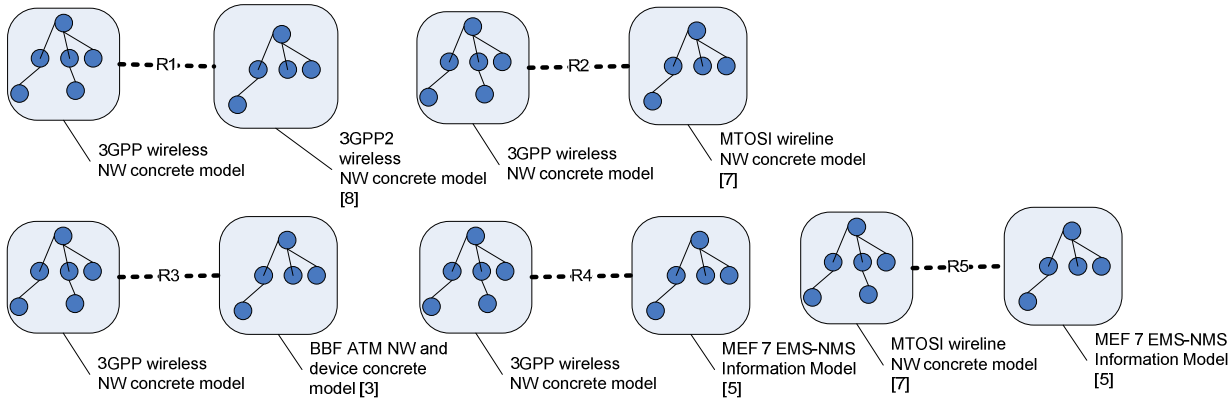


Figure 5.5.3.3-1: Relation between pairs of model components (not involving UIM model component)

Taking the example of a relation between 3GPP model components and BBF ATM model components (i.e. R3 in the figure above): the 3GPP model component would create a necessary 3GPP defined "ExternalIOC" representing one of the classes of "BBF ATM network and device classes". This type of relation is used extensively in the 3GPP IRP framework for the purpose of navigation from one managed domain to another.

6 PLMN management processes

6.1 Process decomposition

The present document details the general aspects of PLMN management. It describes primarily the management processes that collectively support Customer Relationship Management, Service Management&Operations and Resource Management&Operations.

These management processes are based on the widely accepted Enhanced Telecom Operations Map® (or eTOM for short), developed by the TeleManagement Forum. This reference framework for categorizing the business activities that a service provider will use is found in the ITU-T Recommendations M.3050.x series [112].

Figure 3 shows the Operations portion of the eTOM framework decomposed into the Operations Support & Readiness vertical end-end process grouping plus the three Customer Operations vertical end-end process groupings of Fulfilment, Assurance and Billing. The purpose is to show in more detail the predominant processes that need to be involved – integrated and automated – to support the vertical end-to-end, Customer Operations processes of Fulfilment, Assurance and Billing as well as the Operations Support & Readiness processes.

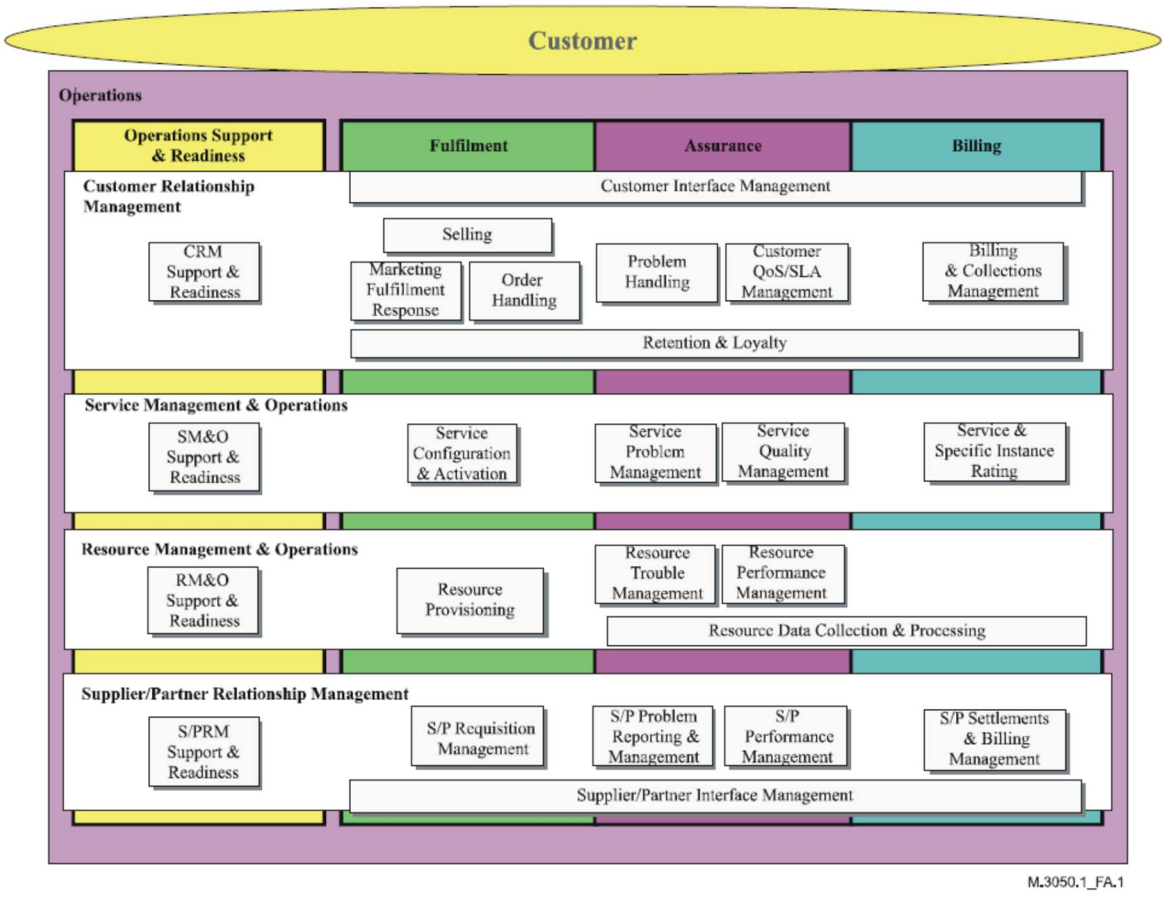


Figure 6.1: Enhanced Telecom Operations Map Business Process Model [113]

The following clauses give a short description of each of the management processes introduced in the "Enhanced Telecom Operations Map®. To see more detailed descriptions refer to ITU-T Recommendations M.3050.x series [112].

6.2 Void

6.3 Void

6.4 Void

6.5 Customer Relationship Management (CRM) processes

Customer Relationship Management (CRM): This horizontal functional process grouping considers the fundamental knowledge of customers' needs and includes all functionalities necessary for the acquisition, enhancement and retention of a relationship with a customer. It is about customer service and support, whether storefront, telephone, web or field service. It is also about retention management, cross-selling, up-selling and direct marketing for the purpose of selling to customers.

CRM also includes the collection of customer information and its application to personalize, customize and integrate delivery of service to a customer, as well as to identify opportunities for increasing the value of the customer to the enterprise.

CRM applies to both conventional retail customer interactions, as well as to wholesale interactions, such as when an enterprise is selling to another enterprise that is acting as the 'retailer'.

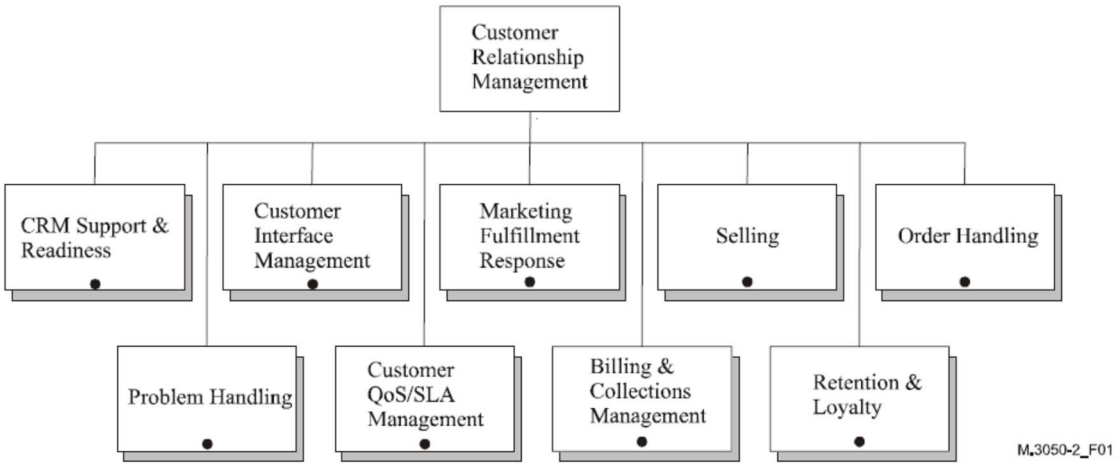


Figure 6.5: Customer Relationship Management decomposition [114]

6.5.1 CRM Support & Readiness

CRM Support & Readiness processes manage classes of products, ensuring that all CRM processes in Fulfilment, Assurance and Billing are supported and able to manage interactions with customers promptly and efficiently. They undertake longer-term trend analysis on product classes in order to establish the extent to which enterprise targets for these product classes are being achieved.

These processes support the operational introduction of new product classes and of additional features and enhancements to existing product classes, and are responsible for conducting operations readiness testing and acceptance. They develop the procedures for the specific Fulfilment, Assurance and Billing processes and keep them up to date. After successful testing, these processes accept the new or enhanced product class and perform a full-scale introduction for general availability.

6.5.2 Customer Interface Management

Customer Interface Management processes are responsible for managing all interfaces between the enterprise and potential and existing customers. They deal with contact management, understanding the reason for contact, directing customer contacts to the appropriate process, contact closure, exception management, contact results analysis and reporting. CRM contact may be related to one or several processes of Service Fulfilment, Service Assurance (service quality management and trouble or problem management) and Billing depending on customer enquiries or contacts.

6.5.3 Marketing Fulfilment Response

Marketing Fulfilment Response processes are responsible for the issue and distribution of marketing collateral (i.e., coupon, premium, sample, toys, fliers, etc.) directly to a customer and the subsequent tracking of resultant leads. These processes include campaign management activities from lead generation to product and literature fulfilment, and hand-off of leads to the selling processes.

6.5.4 Selling

Selling processes are responsible for managing prospective customers, for the qualification and education of the customer and for matching customer expectations to the enterprise's products and services and ability to deliver. These processes also manage the response to customer RFPs.

6.5.5 Order Handling

Order Handling processes are responsible for accepting and issuing orders. They deal with pre-order feasibility determination, credit authorization, order issuance, order status and tracking, customer update on order activities and customer notification on order completion.

6.5.6 Problem Handling

Problem Handling processes are responsible for receiving trouble reports from customers, resolving them to the customer's satisfaction and providing meaningful status on repair and/or restoration activity to the customer.
They are also responsible for customer contact and support in relation to any service-affecting problems detected by the resources or through analysis, including proactively informing the customer and resolving these specific problems to the customer's satisfaction.

6.5.7 Customer QoS/SLA Management

Customer QoS/SLA Management processes encompass monitoring, managing and reporting of delivered vs contractual Quality of Service (QoS), as defined in the enterprise's Service Descriptions, customer contracts or product catalogue. They are also concerned with the performance of the enterprise and its products and services in relation to its Service Level Agreements (SLAs) for specific product instances, and other service-related documents.
They include operational parameters such as resource performance and availability, but also encompass performance across all of a product's contractual or regulatory parameters, e.g., % Completion on Time for Order Requests, time to repair commitments, customer contact performance. Failure to meet a contracted SLA may lead to billing adjustments, which are handled by Billing and Collections Management.

6.5.8 Billing & Collections Management)

Billing & Collections Management processes encompass creating and maintaining a customer's billing account, sending bills to customers, processing their payments, performing payment collections, monitoring the status of the account balance, and the handling of customer generated or systems reported billing and payment exceptions.

These processes are accountable for assuring that enterprise revenue is billed and collected.

6.5.9 Retention & Loyalty

Retention & Loyalty processes deal with all functionalities related to the retention of acquired customers, and the use of loyalty schemes in the potential acquisition of customers. They establish a complete understanding of the needs of the

customer, a determination of the value of the customer to the enterprise, determination of opportunities and risks for specific customers, etc. These processes collect and analyse data from all enterprise and customer contact.

6.6 Service Management & Operations (SM&O) Processes

Service Management & Operations (SM&O): This horizontal functional process grouping focuses on the knowledge of services (Access, Connectivity, Content, etc.) and includes all functionalities necessary for the management and operations of communications and information services required by or proposed to customers.
The focus is on service delivery and management as opposed to the management of the underlying network and information technology. Some of the functions involve short-term service capacity planning for a service instance, the application of a service design to specific customers or managing service improvement initiatives.
These functions are closely connected with the day-to-day customer experience.

The processes in this horizontal functional process grouping are accountable to meet, at a minimum, targets set for Service Quality, including process performance and customer satisfaction at a service level, as well as Service Cost.

The eTOM framework differentiates day-to-day operations and support from planning and development and other strategy and lifecycle processes. This better depicts the structure of an enterprise, especially in an e-business era.

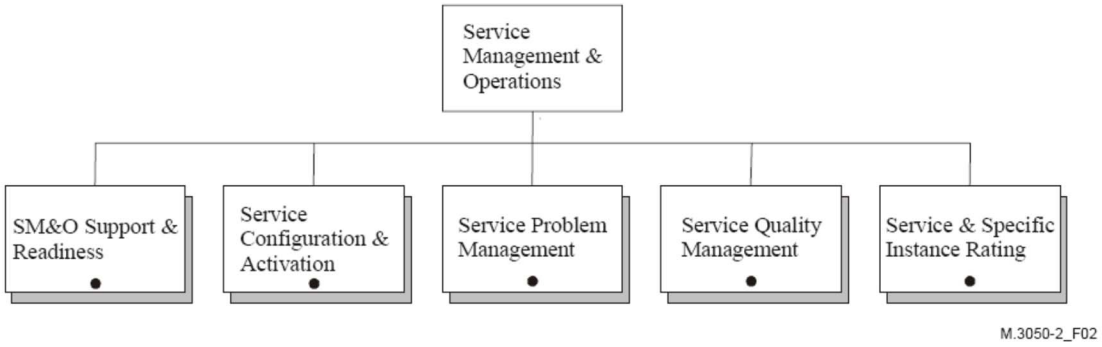


Figure 6.6: Service Management & Operations decomposition [114]

6.6.1 SM&O Support & Readiness

SM&O Support & Readiness processes manage classes of services, ensuring that the appropriate service capacity is available and ready to support the Fulfilment, Assurance and Billing processes in instantiating and managing service instances. This includes but is not limited to:

- Managing the Service Inventory;
- Applying service capacity rules from Infrastructure Lifecycle Management processes;
- Analysing availability and quality over time on service classes, including trend analysis and forecasting;
- Demand balancing in order to maintain service capacity and quality;
- Maintaining rating and tariff information for service classes.

These processes support the operational introduction of new service classes and the enhancement of existing ones and are responsible for conducting operations readiness testing and acceptance. They develop the procedures for the specific Fulfilment,

Assurance and Billing processes and keep them up to date. After successful testing, these processes accept the new or enhanced service class and perform a full-scale introduction for general availability.

6.6.2 Service Configuration & Activation

Service Configuration & Activation processes encompass the installation and configuration of the service for customers, including the installation of customer premises equipment. They also support the reconfiguration of the service (either due to customer demand or problem resolution) after the initial service installation. This can include modifying capacity and reconfiguring in response to requests from other providers.

6.6.3 Service Problem Management

The purpose of the Service Problem Management processes is to respond immediately to customer-affecting service problems or failures in order to minimize their effects on customers, and to invoke the restoration of the service, or provide an alternate service as soon as possible. They encompass the reporting of problems, making a temporary fix or work-around, isolating the root cause and finally recovering the complete functionality of the service and providing information for future enhancements.

6.6.4 Service Quality Management

The purpose of the Service Quality Management processes encompasses monitoring, analysing and controlling the performance of the service perceived by customers. These processes are responsible for restoring the service performance for customers to a level specified in the SLA or other service KQI descriptions as soon as possible.

6.6.5 Service & Specific Instance Rating

Service & Specific Instance Rating processes manage service events by correlating and formatting them into a useful format. These processes include the service level rating of usage information. Investigation of service related billing event problems is also part of these processes. These processes provide information on customer-related and Service-related events to other process areas. This includes reports on non-chargeable Events and overcharged Events and analysis of Event records to identify fraud and prevent further occurrences.

6.7 Resource Management & Operations (RM&O) Processes

Resource Management & Operations (RM&O): This horizontal functional process grouping maintains knowledge of resources (application, computing and network infrastructures) and is responsible for managing all these resources (e.g., networks, IT systems, servers, routers, etc.) utilized to deliver and support services required by or proposed to customers. It also includes all functionalities responsible for the direct management of all such resources (network elements, computers, servers, etc.) utilized within the enterprise. These processes are responsible for ensuring that the network and information technologies infrastructure supports the end-to-end delivery of the required services.
The purpose of these processes is to ensure that infrastructure runs smoothly, is accessible to services and employees, is maintained and is responsive to the needs, whether directly or indirectly, of services, customers and employees.
RM&O also has the basic function to assemble information about the resources (e.g., from network elements and/or element management systems), and then integrate, correlate, and in many cases, summarize that data to pass on the relevant information to Service Management systems, or to take action in the appropriate resource.

In an e-business world, application and computing management are as important as management of the network resources. Moreover, network, computing and applications resources must increasingly be managed in a joint and integrated fashion. To cope with these needs, the eTOM framework includes the Resource Management & Operations process grouping (together with the corresponding Resource Development & Management grouping within SIP), to provide integrated management across these three sets of resources: applications, computing and network. These areas also encompass processes involved with traditional Network Element Management, since these processes are actually critical components of any resource management process, as opposed to a separate process layer.

The RM&O processes thus manage the complete service provider network and subnetwork and information technology infrastructures.

The eTOM framework differentiates day-to-day operations and support from planning and development, and other strategy and lifecycle processes. This better depicts the structure of an enterprise, especially in an e-business era.

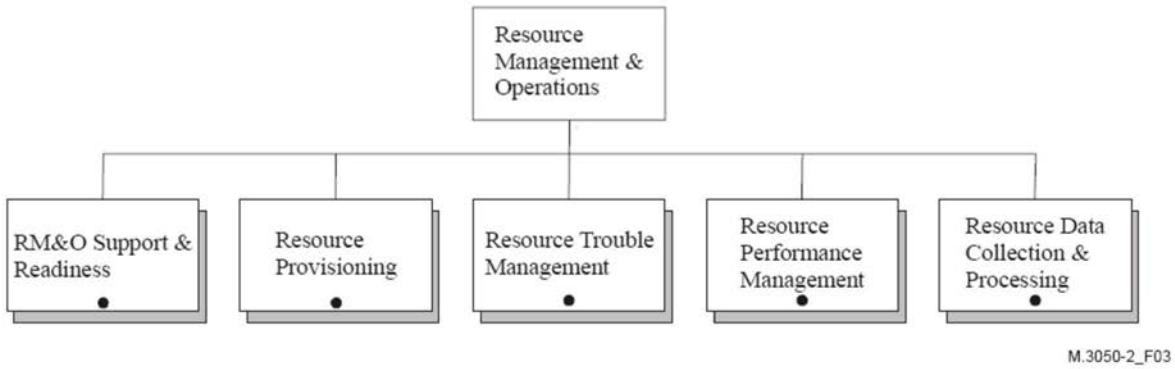


Figure 6.7: Resource Management & Operations decomposition [114]

6.7.1 RM&O Support & Readiness

RM&O Support & Readiness processes manage classes of resources, ensuring that appropriate application, computing and network resources are available and ready to support the Fulfilment, Assurance and Billing processes in instantiating and managing resource instances. This includes, but is not limited to:

- Managing the Resource Knowledge base;

- Configuring the resources and provisioning of logical resources to be able to support specific service classes;

- Analysing availability and performance over time on resources or groups of resources, including trend analysis and forecasting;

- Demand balancing in order to maintain resource capacity and performance;

- Performing pro-active maintenance and repair activities.

These processes support the operational introduction of new resource classes and the enhancement of existing ones and are responsible for conducting operations readiness testing and acceptance. They develop the procedures for the specific Fulfilment,

Assurance and Billing processes and keep them up to date. After successful testing, these processes accept the new or enhanced resource class and perform a full-scale introduction for general availability.

6.7.2 Resource Provisioning

Resource Provisioning processes encompass allocation and configuration of resources to individual customer service instances in order to meet the service requirements. This includes activation as well as testing to ensure the expected performance of the service.

Responsibilities of the Resource Provisioning processes include, but are not limited to:

- Verifying whether appropriate resources are available as part of pre-order feasibility checks;

- Allocating the appropriate resources to support the customer service instance;

- Reserving the resources (if required by the business rules) for a given period of time until the customer confirms the order;

- Possibly delivering the physical resource to the central office or customer premise;

- Configuring and activating physical and/or logical resources, as appropriate;

- Testing the resource to ensure the resource is working correctly and meets the performance requirements implied by the service's Key Quality Indicators;

- Updating of the Resource Inventory Database to reflect that the resource is being used for a specific customer.

6.7.3 Resource Trouble Management

Resource Trouble Management processes are responsible for the management of troubles with allocated resources. The objectives of these processes are to report resource failures, to isolate the root cause and act to resolve them.

Responsibilities of the Resource Trouble Management processes include, but are not limited to:

- Detect, analyse and report Resource Failure Events;
- Fault localization analysis;
- Correcting Resource Faults;
- Resource trouble reporting to amongst others Service Problem Management processes;
- Resource trouble administration to ensure repair activities are assigned and tracked efficiently.

On one hand, resource troubles relate to Problems in the Service and hence the customer domain. On the other hand, they relate to resource failures, which are caused by resource faults.

As such, the Resource Trouble Management processes work with resource failure events received from Resource Data Collection & Processing, resource quality problem notifications from Resource Performance Management, and potential resource failure notifications from Support Resource Trouble Management.

Resource Trouble Management processes perform analysis, decide on the appropriate actions/responses and carry them out. However, these activities need to interact with the Service Problem Management processes, as the latter have a view on service impact.

6.7.4 Resource Performance Management

Resource Performance Management processes encompass monitoring, analysing, controlling and reporting on the performance of resources. They work with basic information received from the Resource Data Collection & Processing processes.

If the analysis identifies a resource quality problem, information will be passed to Resource Trouble Management and/or Service Quality Management. The latter processes are responsible for deciding on and carrying out the appropriate action/response. This may include requests to the Resource Performance Management processes to install controls to optimize the resource performance.

The Resource Performance Management processes will continue to track the resource performance problem, ensuring that resource performance is restored to a level required to support services.

Depending on the resource class, the Resource Performance Management processes might send an abatement message to Resource Trouble Management once the resource performance problem has been cleared.

6.7.5 Resource Data Collection & Processing

Resource Data Collection & Processing processes interact with the resources to collect usage, network and information technology events and performance information for distribution to other processes within the enterprise.
The responsibilities also include processing the data through activities such as filtering, aggregation, formatting and correlation of the collected information before presentation to other processes. Client processes for this information perform usage reporting and billing activities, as well as Fault and Performance analysis of resources and services. These include Resource Performance Management, Service Quality Management and Service & Specific Instance Rating.

6.8 Supplier/Partner Relationship Management (S/PRM) processes

Supplier/Partner Relationship Management (S/PRM): This horizontal functional process grouping supports the core operational processes, both the customer instance processes of Fulfilment, Assurance and Billing and the functional operations processes.

Supplier/Partner Relationship Management (S/PRM) processes align closely with a supplier's or partner's Customer Relationship Management processes. The inclusion of distinct Supplier/Partner Relationship Management processes in the eTOM framework enables the direct interface with the appropriate lifecycle, end-to-end customer operations or functional processes with suppliers and/or partners. The processes include issuing RFPs as part of the buy process, issuing purchase orders and tracking them through to delivery, mediation of purchase orders as required to conform to external processes, handling problems, validating billing and authorizing payment, as well as quality management of suppliers and partners.

It is important to note that when the enterprise sells its products to a partner or supplier, this is done through the enterprise CRM processes, which act on behalf of the supplier or the enterprise in such cases. Supplier/Partner processes only cover the buying of services by the enterprise.

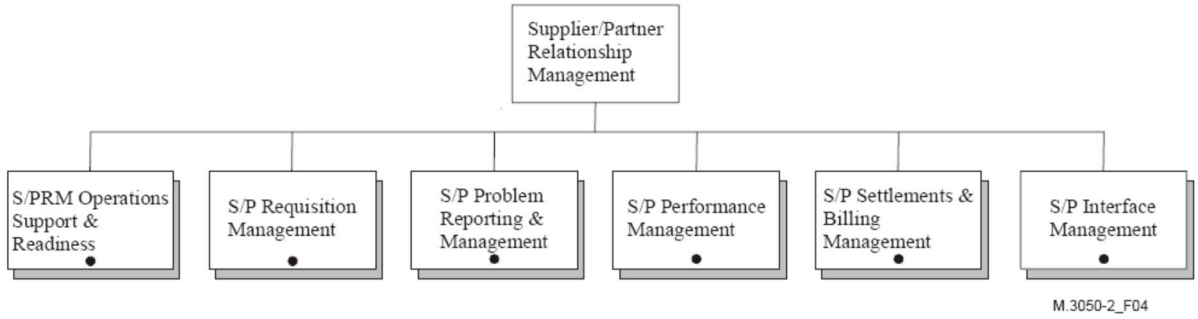


Figure 6.8: Suppler/Partner Relationship Management decomposition [114]

6.8.1 S/PRM Support & Readiness

S/PRM Support & Readiness processes are responsible for ensuring that all necessary facilities related to the interaction with Suppliers and Partners are ready and functioning. Moreover, these processes are responsible for longer-term trend analysis and the resolution of problems related to these facilities.

These processes are also responsible for the operational introduction of S/P products and are responsible for conducting operations readiness testing and acceptance. These processes develop the procedures for the specific Fulfilment, Assurance and Billing processes and keep them up to date. After successful testing, these processes accept the new or enhanced product and perform a full-scale introduction for general availability.

6.8.2 S/P Requisition Management

S/P Requisition Management processes manage requisitions with partners/suppliers to ensure on-time and correct delivery of the product or service requested by the enterprise. This process interfaces with supplier's CRM process Order Handling.

Where several suppliers are available, these processes are responsible for selecting between the alternative suppliers with whom a relationship exists. A specification for the service component is received and the range of contracted suppliers surveyed to select the most cost-effective (cost/time trade-off).

6.8.3 S/P Problem Reporting & Management

S/P Problem Reporting & Management processes manage problems associated with supplier/partner interactions, whether identified within the enterprise or as notified by the supplier. The processes issue trouble reports or trouble

tickets to supplier and partner organizations within the value chain, track them, and ensure timely and correct restoration and repair. These S/P Problem Reporting and Management processes interface with the supplier's CRM process of Problem Handling.

6.8.4 S/P Performance Management

S/P Performance Management processes track, measure and report supplier and partner performance and initiate action with the supplier/partner where this is required to restore performance. These S/P Performance Management processes interface with the supplier's CRM process of Customer QoS/SLA Management.

6.8.5 S/P Settlements & Billing Management

For a value network, and particularly for service providers, settlements and billing management is complex. In many cases, the supplier cost can be the largest single cost and incorrect settlement or billing can mean the difference between profit and loss. S/P Settlements & Billing Management processes manage all settlements and billing for the enterprise, including bill validation and verification and payment authorization. These S/P Settlements and Billing Management processes interface with the supplier's Customer Relationship Management process of Billing and Collection Management.

6.8.6 S/P Interface Management

S/P Interface Management processes manage the contacts between the enterprise and its current or future suppliers/partners for products or services. These processes are basically contact management and tracking processes. These S/P Interface Management processes interface with the CRM process of Customer Interface Management.

7 PLMN management functional architecture

7.1 TM architectural aspects

The basic aspects of a TM architecture, which can be, considered when planning and designing a TM are:

- the functional architecture;
- the information architecture;
- the physical architecture.

The management requirements from the business needs are the base for the functional architecture, which describe the functions that have to be achieved. The information architecture defines what information that has to be provided so the functions defined in the functional architecture can be achieved. The physical architecture has to meet both the functional architecture and the information architectures. These relationships are shown in figure 5.

The present document addresses the functional architecture. The physical architecture is addressed in TS 32.102 [101].

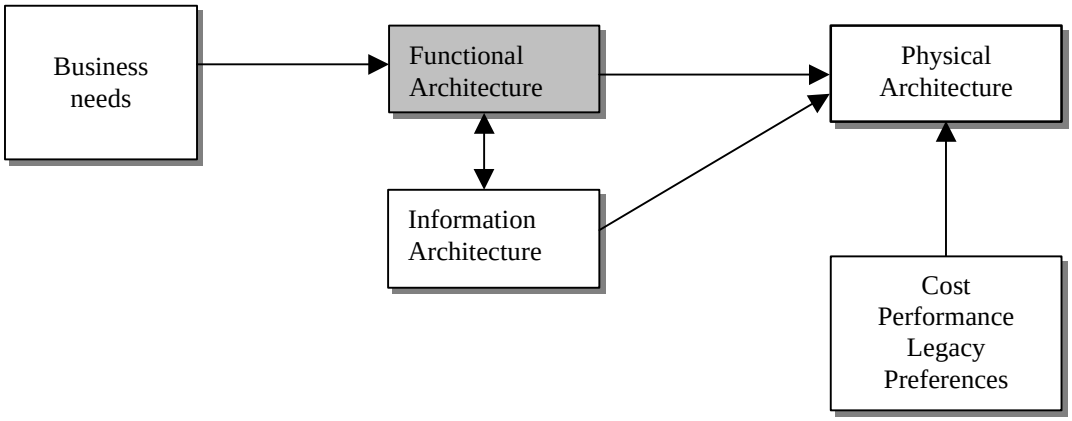


Figure 4: Architectural relationship

All management processes have functions in several management areas. By identifying only those processes and interfaces relating to a certain management function, for example performance management, it is possible to take a slice through the Enhanced Telecom Operations Map that details the functional architecture for performance management, this will be the approach taken by the present document.

The management functions are:

- Performance management;
- Roaming management;
- Fraud management;
- Fault management;
- Security management;
- Software management
- Configuration management;
- Accounting management;
- Subscription management;
- Quality of Service (QoS) management (see informative annex D);
- User equipment management.

The 3GPP IRP methodology focuses on providing the definitions for the O&M operations and notifications needed to support the business requirements provided by the eTOM framework for such management functions.

7.2 Performance Management

7.2.1 Overview

An initial view of Performance Management is described in [105]. This shows an example decomposition of Performance Management processes to identify essential information flows. It shows a slice through the Telecom Operations Map from a Performance Management point of view. This slice is applicable to Mobile Networks and other networks. Although the "slice" or view is quite large, it does not contain all interfaces or process activities that are related to Performance Management. It does however show the main processes and interfaces involved in Performance Management. Please refer to [105] for further detail.

7.2.2 Standardisation objectives

During the lifetime of a 3GPP system, its logical and physical configuration will undergo changes of varying degrees and frequencies in order to optimise the utilisation of the network resources. These changes will be executed through network configuration management activities and/or network engineering, see TS 32.600 [54].

Many of the activities involved in the daily operation and future network planning of a 3GPP system require data on which to base decisions. This data refers to the load carried by the network and the grade of service offered. In order to produce this data performance measurements are executed in the NEs, which comprise the network. The data can then be transferred to an external system, e.g. an Operations System (OS) in TMN terminology, for further evaluation. The purpose of the present document is to describe the mechanisms involved in the collection of the data and the definition of the data itself.

The Performance Management functional area concerns the management of performance measurements and the collection of performance measurement data across a 3GPP system. It defines the administration of measurement schedules by the Network Element Manager (EM), the generation of measurement results in the Network Elements (NEs) and the transfer of these results to one or more Operations Systems, i.e. EM(s) and/or Network Manager(s) (NM(s)).

The management requirements have been derived from existing telecommunications operations experience. The management definitions were then derived from other standardisation work so as to minimise the re-invention factor. References are given as appropriate.

The objectives of the present document are:

- To provide the descriptions for a standard set of measurements;
- To produce a common description of the management technique for measurement administration and result accumulation; and
- To define a method for the bulk transmission of measurement results across a management interface.

The definition of the standard measurements is intended to result in comparability of measurement data produced in a multi-vendor 3GPP system, for those measurement types that can be standardised across all vendors' implementations.

As far as possible, existing standardisation in the area of Performance Management is re-used and enhanced where particular requirements, peculiar to the mobile telephony environment, have been recognised.

Performance management is further specified in TS 32.400-series [53].

7.3 Roaming management overview

Roaming is a service provided by Mobile Service Providers. Customers of a Home Service Provider may use the infrastructure of another, a Serving Service Provider (see figure 5) to give its customer the ability to make calls when outside the home service provider' s territory. The goal is to have a customer receive the same service (or as close to the same service) when travelling in an area supported by another network as the customer receives when in their home service provider's area. Please refer to [105] to see an example implementation with more detail.

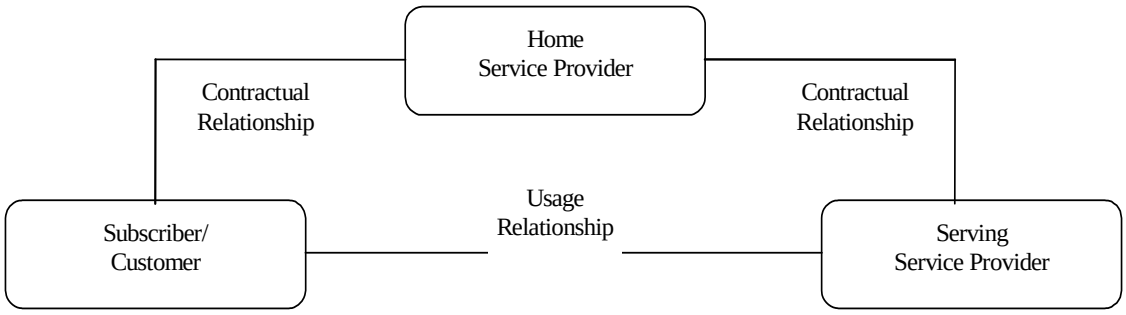


Figure 5: Relationships between Subscriber, Home and Serving Service Provider

7.4 Fraud management overview

Fraud and all the activities to detect and prevent fraud are quite common to any network. Nonetheless, mobility and roaming, two integral mobile services, make fraud detection and fraud prevention more complicated and more urgent. The mobile service provider does not know the location of the "end of the wire," which would lead to the home of a fraudulent customer. For roaming, the situation is demonstrably worse. For a roaming visitor the caller is not the service provider's customer and therefore, the service provider does not have complete information to assess fraud. In the reverse case, the service provider has little control when its customers are roaming, e.g., potentially going over credit limits or using service after being suspended. In this case, the fraudulent customer uses the network facilities of another provider (the serving service provider) meaning the home service provider has to rely on the serving service provider for some level of fraud protection support. This means to a large extent that fraud prevention is largely out of the control of the home service provider when one of its customers roams on another network and out of the control of a serving service provider when being visited by another provider's roamer. Please refer to [105] to see an example implementation with more detail.

7.5 Fault Management

7.5.1 Overview

Fault Management is accomplished by means of several processes/sub-processes like fault detection, fault localisation, fault reporting, fault correction, fault repair, etc. These processes/sub-processes are located over different management layers, however, most of them (like fault detection, fault correction, fault localisation and fault correction) are mainly located over the Network Element and Network Element Management layers, since this underlying network infrastructure has the 'self healing' capabilities.

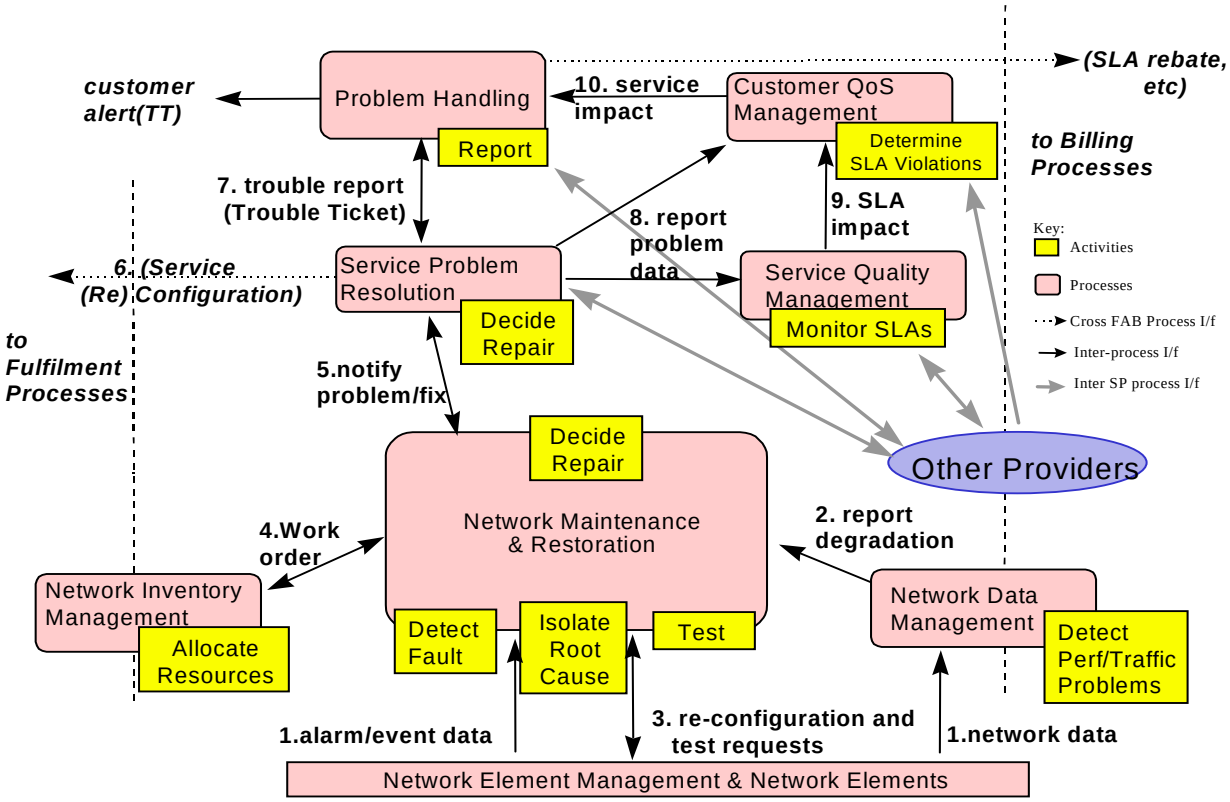
It is possible, however, that some faults/problems affecting the telecom services are detected within the "Network and Systems Management" layer, by correlating the alarm/events (originated by different Network Elements) and correlating network data, through network data management.

Network data management logically collects and processes performance and traffic data, as well as usage data.

While the Fault Management triggered within the Network Element and NE management layers is primarily reactive, the Fault Management triggered within the Network and Systems Management layer is primarily proactive. Meaning triggered by automation rather than triggered by the customer; and this is important for improving service quality, customer perception of service and for lowering costs.

Focusing on the Network and Systems Management layer, when a fault/problem is detected, no matter where and how, several processes are implicated, as described in figure 6.

Figure 6 taken from the Telecom Operations Map [100] shows an example of how Fault Management data can be used to drive an operator's service assurance process. Service assurance then becomes primarily proactive, i.e. triggered by automation rather than triggered by the customer. It is argued that this approach is crucial to improving service quality, customer perception of service and for lowering costs.



NOTE: Flow "3." has been added in the present document.

Figure 6: Service Assurance Process Flow (* imported from [100])

TOM assurance activities (and their associated interfaces) shown in figure 6 can be associated with ITU-T TMN service components from TS 32.111-series [3] according to table 1:

Table 1

ITU-T TMN Service Component TS 32.111-x [3]	TOM Network Management Assurance Activities
Alarm Surveillance	Detect Fault
Fault Localisation	Isolate Root Cause
Fault Correction	Decide Repair / Allocate Resources
Testing	Test

The TOM assurance example shown in figure 6 also recognises that Performance Management data can also be used to detect network problems.

The TOM assurance example also adds some detail to the Service Management Layer by showing how activities such as determining and monitoring Service Level Agreements (SLAs) and trouble ticket reporting are interfaced to the Network Management layer.

7.5.2 Standardisation objectives

A 3GPP system is composed of a multitude of Network Elements (NE) of various types and, typically, different vendors, which inter-operate in a co-ordinated manner in order to satisfy the network users' communication requirements.
The occurrence of failures in a NE may cause a deterioration of this NE's function and/or service quality and will, in severe cases, lead to the complete unavailability of the respective NE. In order to minimise the effects of such failures on the Quality of Service (QoS) as perceived by the network users it is necessary to:

- detect failures in the network as soon as they occur and alert the operating personnel as fast as possible;
- isolate the failures (autonomously or through operator intervention), i.e. switch off faulty units and, if applicable, limit the effect of the failure as much as possible by reconfiguration of the faulty NE/adjacent NEs;
- if necessary, determine the cause of the failure using diagnosis and test routines; and
- repair/eliminate failures in due time through the application of maintenance procedures.

This aspect of the management environment is termed "Fault Management" (FM). The purpose of FM is to detect failures as soon as they occur and to limit their effects on the network Quality of Service (QOS) as far as possible. The latter is achieved by bringing additional/redundant equipment into operation, reconfiguring existing equipment/NEs, or by repairing/eliminating the cause of the failure.

Fault Management (FM) encompasses all of the above functionalities except commissioning/decommissioning of NEs and potential operator triggered reconfiguration (these are a matter of Configuration Management (CM), cf. TS 32.600 [54]).

FM also includes associated features in the Operations System (OS), such as the administration of a pending alarms list, the presentation of operational state information of physical and logical devices/resources/functions, and the provision and analysis of the alarm and state history of the network.

Fault management is further specified in TS 32.111-series [3].

7.6 Security Management

7.6.1 Overview

This clause describes an architecture for security management of the TMN that is divided into two layers, as shown in figure 7. No individual layer is dependent on any specific technology in the other one.

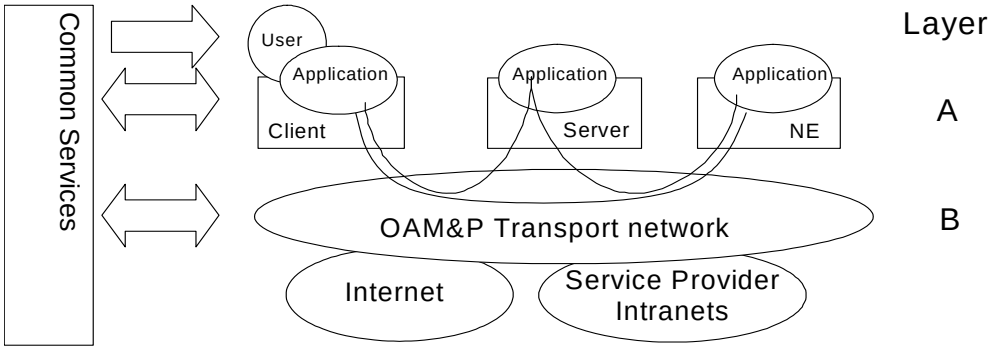


Figure 7: Security Management architecture

7.6.1.1 Layer B - OAM&P Transport IP Network

Some Service Providers might build their OAM&P transport network as a completely private, trusted network. In the normal case though, the OAM&P transport network should be regarded as partly insecure due to its size, complexity, limited physical security and possible remote access from dial-up connections or from the Internet. The only security service provided then is that the OAM&P transport network when based on IP is logically separated from the Internet. For IP based transports infrastructure aspects on security are handled to the extent possible utilizing IP classic features (addressing schemes, DNS, DHCP, BOOTP, protection with firewalls etc.).

Additionally, a trusted IP-environment to the application level might be provided, e.g. an environment with no masquerading IP-hosts and where potential intruders cannot communicate. One way to accomplish such a secure DCN is to use IP security mechanisms (IPSec; see IETF RFC 2401 [7]) to achieve authentication of IP hosts (servers, gateways, Network Elements) and optional encryption of OAM&P traffic. Note however that the secure DCN does not authenticate users.

7.6.1.2 Layer A - Application Layer

On this layer we find Telecom Management applications performing their tasks in the normal management functional areas. Managed objects residing in the network resources are often accessed or manipulated.

Layer A provides authentication of users ensuring that every party involved in OAM&P traffic is securely authenticated against every other party. The implementation of the authentication service supports "single log-on" (a user only has to log-on once to get access to all OAM&P applications in the network) and "single point of administration" (an administrator only needs to maintain a user and his/her profile in one place).

Layer A also provides authorization (access control) - to verify if a user is authorized to perform a certain operation upon a specified target object at a given time. In addition, it addresses the use of signing and logging of events. Logging of events here means "logging of actions" (not necessarily logging of ALL actions) to be able to check "who did what". At least all "critical" actions (configurations etc.) should be logged.

Interface definitions addressing authentication and authorization are needed. Also note that layer A requires confidentiality. Layer B may provide this service. If not, layer A instead has to provide it itself.

7.6.1.3 Common Services

In common services we find the security infrastructure components:

- Directory (for storage of user information, certificates, etc.);
- PKI (Certificate Authority, Registration Authority, Public Key Certificate, etc.).

Layer A relies on, and interacts with, the Common Services through distribution of certificates and keys, authentication of users, authorization, utilities for security administration (setting access rights), etc.

NOTE: Layer B does not necessarily interact with Common Services for security management purposes. The arrows in figure 7 simply indicate the possible use of common services for Configuration Management.

7.7 Software Management

7.7.1 Overview

This clause describes the software management process for 3rd Generation networks. Two main scenarios are considered:

1) Main Software Management process: It covers requesting, acceptance, installation, monitoring, documenting, database updating and feedback to the vendor for managing software. The sub-processes are valid for complete software releases and software patches for fault correction of the Network Elements and even element managers.

2) Software Fault Management: Its emphasis is on network monitoring and handling faults, which are caused by software malfunctions.

7.7.1.1 Main Software Management process

The main focus is the management of new software releases and correction patches. Importance is placed integrating new software into a network with out causing unnecessary service disruptions and maintaining high levels of quality for the network. The main steps in the software management process are:

- Delivery of software from the vendor.
- Delivery of the software to local storage in the Network Elements and/or element managers.
- Validation of the software to ensure that the Software is not corrupt.
- Activation of the software to an executable state.
- Validation of the software to ensure that it runs correctly.
- Acceptance or rejection of the software, depending on the outcome of the validation. (A rejection of the software implies a reversion to a previous software version).

Figure 8 shows an example of how these steps may be realized in terms of activities involving the processes defined in the Telecom Operations Map. However, alternative sequences may exist. For example, increased automation may cause step 3 to be omitted. Instead, a vendor certification activity could be run for a series of software releases or patches.

The following list is an explanation to the steps in figure 8.

1) Based on inputs from customer care interactions and marketing research, a network operator will establish new feature requirements. These requirements are sent to the vendor in the form of a feature request.

2) The vendor delivers a new software release/correction with the corresponding documentation and installation procedure to the network operator. It should be noted that when a network operator utilises equipment from more than one vendor, this process runs as multiple parallel processes.

3) A service quality management department of the network operator receives and reviews the software. Upon approving the software for installation, the software is sent to the network-provisioning department.

4) Installation Task:

   a) The software is installed in the appropriate Network Elements and/or element managers by network provisioning.

   b) Installation information is sent to the network maintenance and restoration department to inform them of pending changes in the network.

   c) Installation information is sent to the customer care centre to inform them of pending changes in the network.

5) Installation Test and Validation:

   a) Once the software has been installed, network provisioning performs tests to check and ensure that the new software is working properly.

b) In addition to the checks that are performed by network provisioning, network maintenance and restoration could also detect malfunctions within and outside the updated Network Element (NE).

c) Should network maintenance and restoration detect a problem within the updated Network Element (NE), then network provisioning is informed to decide on further actions.

6) Successful Installation Result:

a) Upon successful installation of the software, the service quality management department is informed.

b) A report is sent to network maintenance and restoration to inform them that the software will remain implemented in the network. At this point the documentation library and software database is updated.

c) The network data management department is informed over the changes in the network.

7) Negative Installation Result:

a) If the installation fails, network provisioning performs a "fallback", i.e. remove the new software and insure that the Network Element (NE) is running properly on the old software.

b) A report containing the negative results and findings will be sent to service quality management and at the same time to network maintenance and restoration.

8) Once the installation procedure has been ended, the network maintenance and restoration department closely monitors the affected Network Element (NE) to ensure proper performance.

9) Service quality management will send feedback to the vendor as to the positive or negative results of the installation.

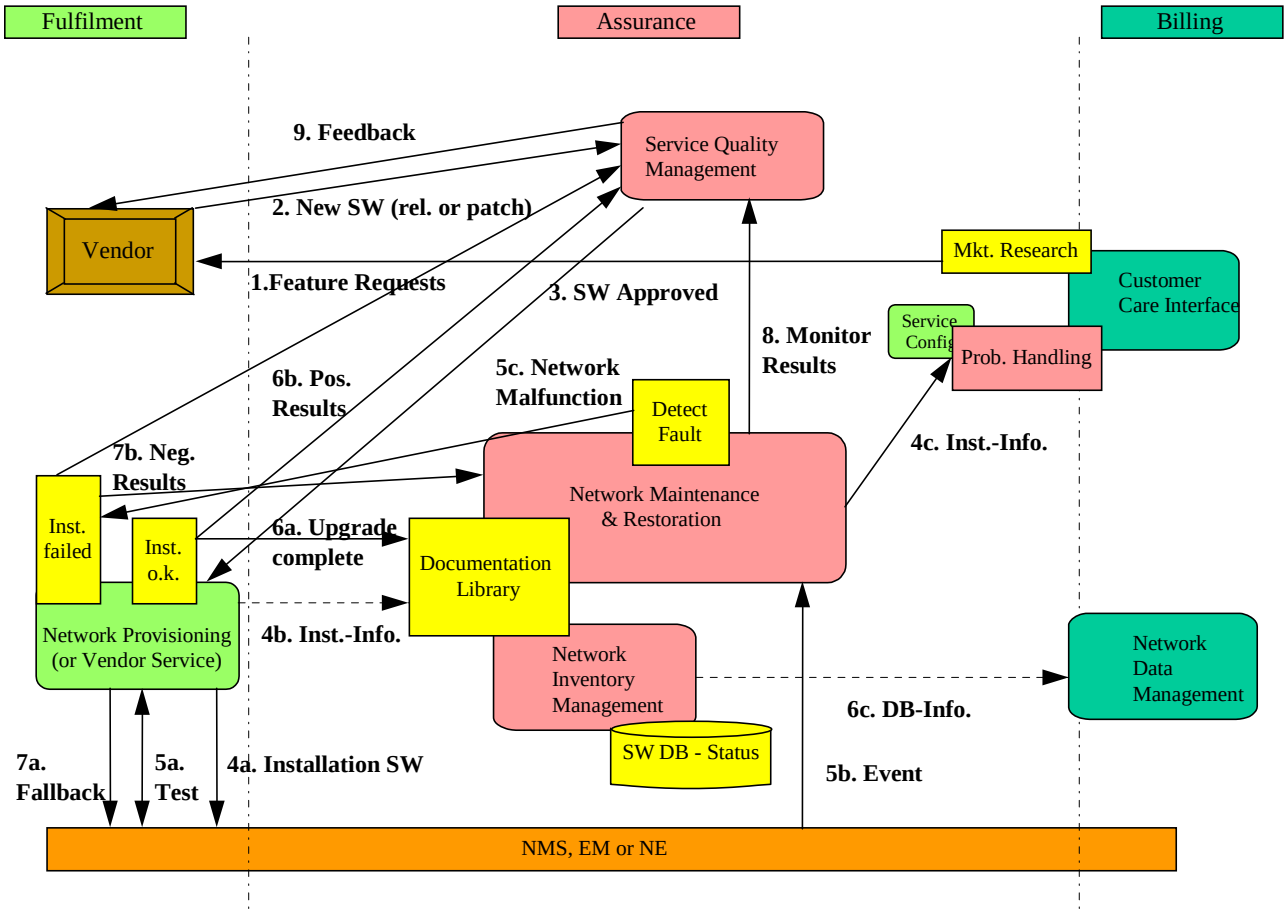


Figure 8: Main Software Management process

7.7.1.2 Software Fault Management

Software Fault Management involves the following steps:

- Detection of Software malfunctions in the network.
- Problem resolution. The origin of the malfunction is determined and corrective action is decided. The corrective action can be one of the following:
  - Reversion to an earlier software version. This can imply both load and activation of the earlier software.
  - Load and activation of correction software, according to clause 8.7.1.
  - Re-activation of current software.

Figure 9 shows an example of how these steps may be realized in terms of activities involving the processes defined in the Telecom Operations Map.

The following list is an explanation to the steps in figure 9.

1) The network maintenance and restoration department detects an event or an alarm/fault from the Network Element (NE).
2) Problem solving and informing customer care:
   a) The alarm is forwarded to the service problem resolution department for corrective actions and it is determined that the problem is caused by a software defect.
   b) In parallel the Customer Care Centre is informed, if the malfunction of the network may have impact on customers.
3) The service problem resolution department informs problem handling and subsequently the customer care centre over service impairments with in the network.
4) Problem handling reports to the service quality management department. The service disturbance is described within the report.
5) Service quality management checks the current software level of the affected Network Element with the network inventory management department.
6) If major network disturbances still appear the Service Quality management decides to fallback to a stable Software version (maybe some time after a new Software installation) and requests Network Provisioning.
7) a+b): Network Provisioning performs the fallback and informs Network Maintenance and Inventory.
8) Service quality management sends a request for a software correction to the vendor.
9) The vendor sends a new software release or correction to the network operator. The rest of the procedure can be followed in the main software management process.

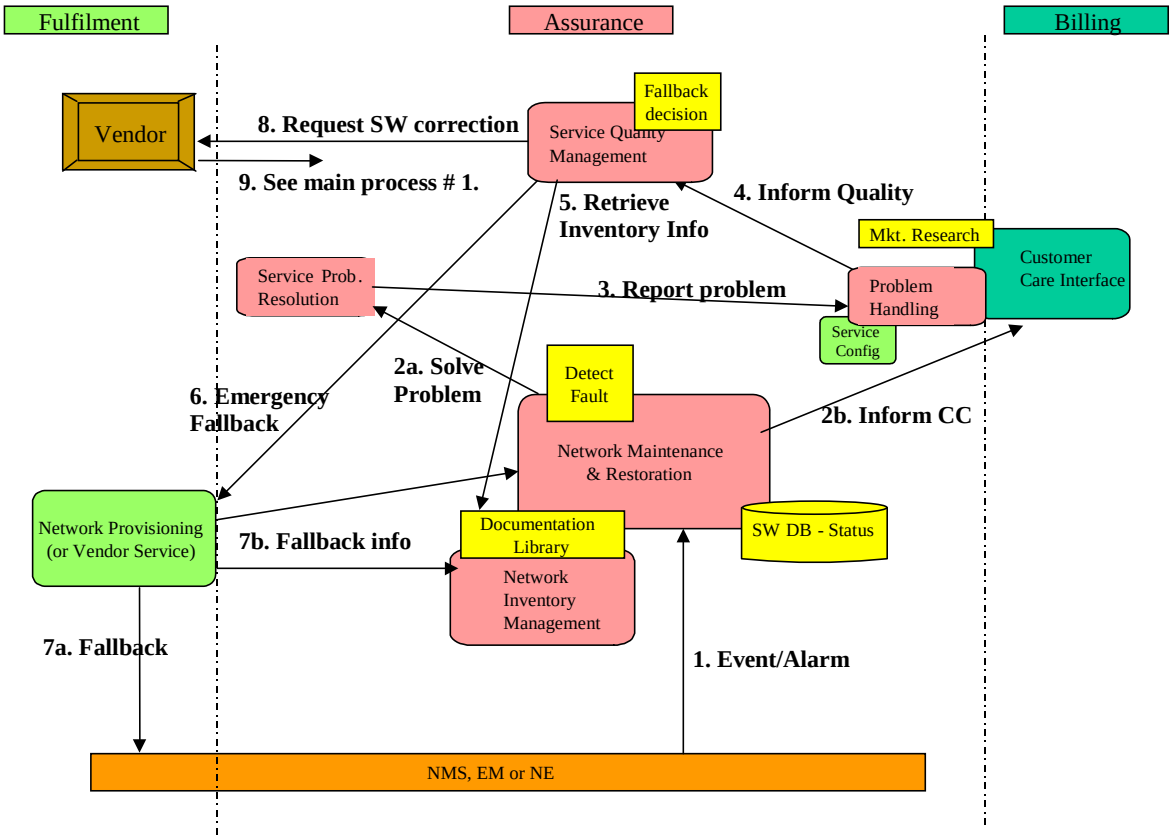


Figure 9: Software Fault Management

7.8 Configuration Management

A variety of components will make up an operator's actual implementation of a 3GPP system. Since it is an explicit goal of the standardisation effort within 3GPP to allow mix and match of equipment from different vendors, it is expected that many networks will indeed be composed of multiple vendors' equipment. For an operator to be able to properly manage this diverse network, in order to provide the quality of service expected by his customers, it is essential to standardise the Configuration Management for 3GPP systems at least to an extent that the operation of the multi-vendor network will be possible effectively and efficiently. Within the scope of Configuration Management, a distinction has to be made between those aspects targeting single Network Elements (NE management level) and those that are also, or exclusively, relevant for some part or the entire network (Network Management level).

Configuration Management is further specified in TS 32.600 [54].

7.9 Accounting Management

3GPP charging data descriptions will be based on the requirements specified in TS 22.115 "Service aspects; Charging and Billing" [51] and on the charging principles outlined in TS 32.200 "Charging management; Charging Principles" [55]. The main content of 3GPP charging data descriptions will be:

- Layout and formats of Charging Data Records (CDRs) for the 3GPP core network nodes (circuit, packet switched and IP Multimedia) and service nodes (e.g. MMS);
- Data generation dependent on call states, chargeable events and TS 22.115 [51] service requirements;
- Formal description of the CDRs format in ASN.1 (ITU-T Recommendation X.680-1997 [49]) and definition of a file transfer mechanism (FTP).

7.10 Subscription Management

Subscription Management (SuM) is a feature that permits Service Providers, Value Added Service Providers and Mobile Operators to provision services for a specific subscriber. The feature is necessary to allow Service Providers and Operators to provision, control, monitor and bill the configuration of services that they offer to their subscribers. SuM focuses on the OAM processes to manage subscription information. These correspond to the 'Fulfilment' Process areas of the TeleManagement Forum Telecom Operations Map [100].

SuM is an area of service operation management that sets a complex challenge for Service Providers and Operators in their support of new or existing subscribers during their every day network operation.

In GSM solutions the main repository of the subscription information is in the Home Locations Register (HLR). However the management and administration interfaces for controlling this information is proprietary to each vendor. The use of proprietary interfaces is inconvenient for those Operators using multiple vendors' equipment since their provisioning systems have to accommodate multiple proprietary interfaces, which perform essentially identical functions. Moreover, it makes it more difficult to generate customer self care applications that allow subscribers to provision, and amend subscription data.

The 3GPP environment requires more complex service delivery mechanisms than in GSM and SuM is no longer simply an internal matter for a single operator but a capability that is achieved by linking together features across multiple Service Providers and Operators Operations Support Systems (OSS). Historically, the services provided by Operators have been defined within standards groups such as ETSI or 3GPP. With the advent of Open Services Access (OSA) being adopted by 3GPP the User Service Definitions will be replaced by Service Capabilities traded amongst Service Providers and Network Operators. This will allow Operators and Service Providers to define customized service environments that roam with users as they move amongst networks - this is the Virtual Home Environment (VHE) 3GPP TR 22.121 [56]. This customized service environment means that subscription information is held in a number of locations including the Home Network, the Visited Network, the User Equipment, Application VASP Equipment (e.g. servers accessed by the subscriber for content and information based services) and the Operations Systems of the Service Providers, and Operators supporting the subscriber's service subscription.

Service delivery and support across multiple vendors' solutions and organizations is a feature of other industries, and the solutions adopted are secure supply chain solutions based upon mainstream e-commerce principles, methods and technologies.

There is a relationship between this feature and the PS Domain, CS Domain, IP Multimedia Subsystem (IMS), Authentication Center (AuC), Open Services Access (OSA) and Generic User Profile (GUP) documented in other 3GPP specifications.

The conceptual model for SuM is illustrated in figure 10.

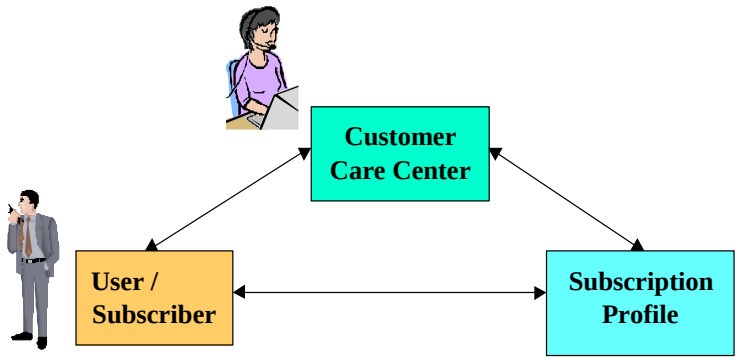


Figure 10: High level view of Subscription Management (SuM)

SuM is concerned with provisioning the subscription profile throughout all the systems and trading partners needed to realize the customer service, SuM provides specifications that define the interfaces and the procedures that interconnect the three points of the SuM triangle: Customer Care Center, the User and the network (s) where the Subscription profile resides (such as HSS, USIM, etc.).

The SuM requirements are described in more detail in 3GPP TS 32.140 [57], The SUM Architecture is described in 3GPP TS 32.141 [58].

7.11 Subscriber and Equipment Trace Management

Subscriber and Equipment Trace Management is a Feature that allows a Network Operator to activate/deactivate from the Network Management system the tracing of a particular subscriber within the network. Once activated the trace activity is reported back to the Network Management system. It will be possible to request activation of a trace from different Network Elements (via the appropriate Element Management Functionality) depending on the operator's requirements.

7.12 OAM&P of the PLMN "Management Infrastructure"

As described earlier in the present document, each PLMN organisation has a management infrastructure consisting of a collection of systems (computers and telecommunications) - a TMN in ITU-T parlance - used to manage its network. Though this management network is logically distinct from the PLMN , the operations systems and supporting data communications network comprising it have the same management needs as described for network elements and where possible should be managed using the same principles and similar management processes and functionality.

7.13 Service Level Trace Management

Service Level Trace Management is a feature that allows a Network Operator to activate/deactivate from the Network Management system the tracing of a particular subscriber and the service that they are consuming within and across an IP Multimedia Subsystem (IMS). Once activated the trace activity is reported back to the Network Management system. It is possible to request activation of a trace from different Network Elements including the UE (via the appropriate Element Management Functionality) depending on the operator's requirements.

The activation/deactivation and reporting interface for Trace Management between the Network Management and Element Management Systems is specified in the Trace IRP.

7.14 Management of QoE measurement collection

Management of QoE measurement collection is a feature that allows a network operator to activate/deactivate from the network management system the collection of QoE information (DASH or MTSI) from applications that are consumed in the UE. When the application has recorded QoE information, it is sent to a specified destination. It is possible to request activation of QMC from an specified area in the network.

The activation/deactivation and reporting interface for the QMC between the network management and element management systems is specified in the Management of Quality of Experience (QoE) measurement collection IRP.

Annex A (normative): 3GPP Management-application-layer-protocols

The valid Management-application-layer-protocols for 3GPP are:

- CORBA IIOP (see references [8] and [52]);
- NETCONF (see reference [118]);
- SNMP (see reference [6]);
- SOAP (see references [108] and [109]).

The valid Management-application-layer-protocols for bulk & file transfer are:

- FTAM (see references [13] – [19]);
- ftp (see reference [4]);
- tftp (see reference [5]);
- sftp (secure ftp).

NOTE: sftp is an implementation of ftp that uses SSL (SSH-1 or SSH-2 transport protocol) to provide a secure ftp. There are many commercial and open source implementations available. An IETF Secure Shell working group exists, whose goal is “to update and standardize the popular SSH protocol”. Currently no IETF RFCs are available, however a number of IETF drafts can be found at the working groups' home web site: http://www.ietf.org/html.charters/secsh-charter.html.

The valid Management-application-layer-protocol for Home NodeB Management Interface Type 1 and Home eNodeB Management Interface Type 1 is:

- TR-069 (see reference [115])

The valid Management-application-layer-protocols for bulk & file transfer for Home NodeB Management Interface Type 1 and Home eNodeB Management Interface Type 1 are defined in TR-069 [115].

Annex B (normative): 3GPP management network layer protocols

The valid network layer protocols for the management of 3GPP are:

- IP (see reference [48];
- X.25 (see reference [22]).

NOTE 1: IP is the recommended networking protocol.

NOTE 2: Normative references relating to ISO Transport over TCP-IP are [46] and [47] and ISO Transport over X.25 are [43] - [45].

Annex C (normative): 3GPP management IRP Solution Sets

The valid IRP Solution Sets for the management of 3GPP on the Itf-N and Itf-P2P interfaces are:

- CORBA (IDL);
- SOAP (WSDL).

The SOAP Solution Set is based on definitions set forth in WS-I Basic Profile 1.1 [116], and consisting of:

- WSDL 1.1 [117];
- SOAP 1.1 [108].

IRPAgents may support only one Solution Set. IRPManagers shall support all Solutions Sets that are supported by IRPAgents they communicate with.

Annex D (informative): QoS Management

D.1 Overview

QoS Management, from an OAM&P perspective, in 3GPP systems primarily consists of two functional areas: QoS policy provisioning and QoS monitoring. QoS Policy Provisioning is the process of configuring and maintaining selected Network Elements with QoS policies that are created based upon customer SLAs and observed network performance. QoS Monitoring is the process of collecting QoS performance statistics and alarms; this data is then used to generate analysis reports for making changes/upgrades to the network. The detailed relationship between SLA Management and QoS Provisioning and Monitoring is for future study. A conceptual breakdown of QoS Management is shown in figure D.1.

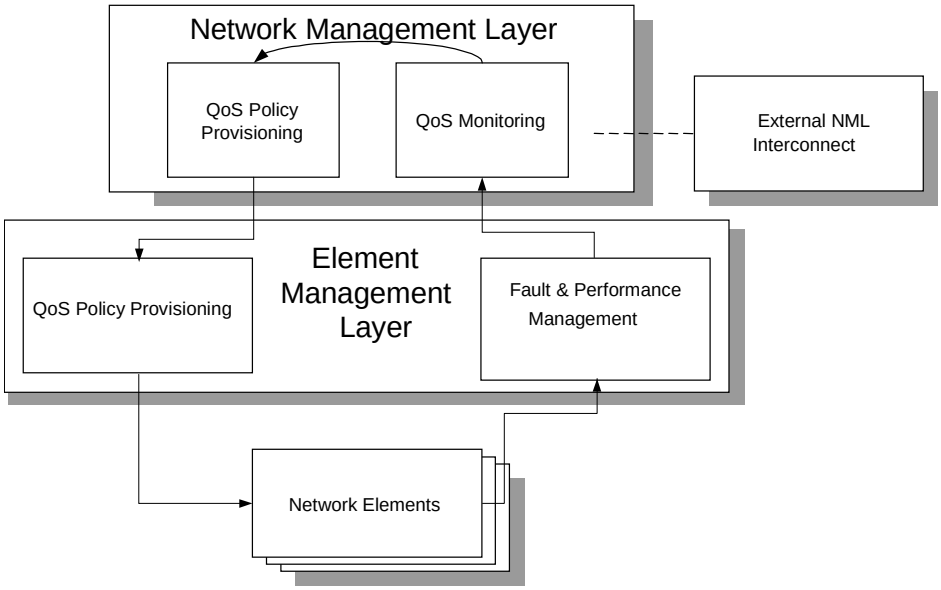


Figure D.1: QoS Management

The following clauses provide descriptions of QoS Provisioning and Monitoring.

It should be noted that the same descriptions could apply to other Policy Management instantiations, e.g. Security and Service Provisioning.

D.2 QoS Provisioning

D.2.0 Introduction

In the 3GPP systems, multiple network domains **must** inter-work in order to provide the end-to-end quality of service required by end-user applications. To add to this complexity, there are many classes of Network Elements from many network infrastructure suppliers, each of which require configuration in a consistent manner in order to the network operator's QoS objectives. Within each Network Element, there are many QoS functions (such as Admission Control, Policers, Shapers, Queue Manager and Scheduler), which **must** be configured.

In order to configure these heterogeneous networks so that they can deliver the desired QoS, the operator needs a management solution that meets the following high-level requirements:

- *Automation* of management tasks.
- *Centralized* management with fewer classes of management interface.
- *Abstracted* (or simplified) management data.
- *End-to-End* provisioning of the network.
- *Consistent and uniform* provisioning across all Network Elements.
- *Standards-based* solution in order to allow *inter-operability* at Network Element and OSS level.
- *Scalable* solution for large networks.

The IETF Policy Management Framework has been designed with these requirements in mind

The various standards that apply to QoS Policy Provisioning as described in the following clauses are listed in D.4.1. At time of publication of the present document there are also a significant amount of IETF Drafts available on the subject at http://www.ietf.org,

D.2.1 Conceptual Architecture

The conceptual architecture for a policy-based QoS Management System is shown in figure D.2.

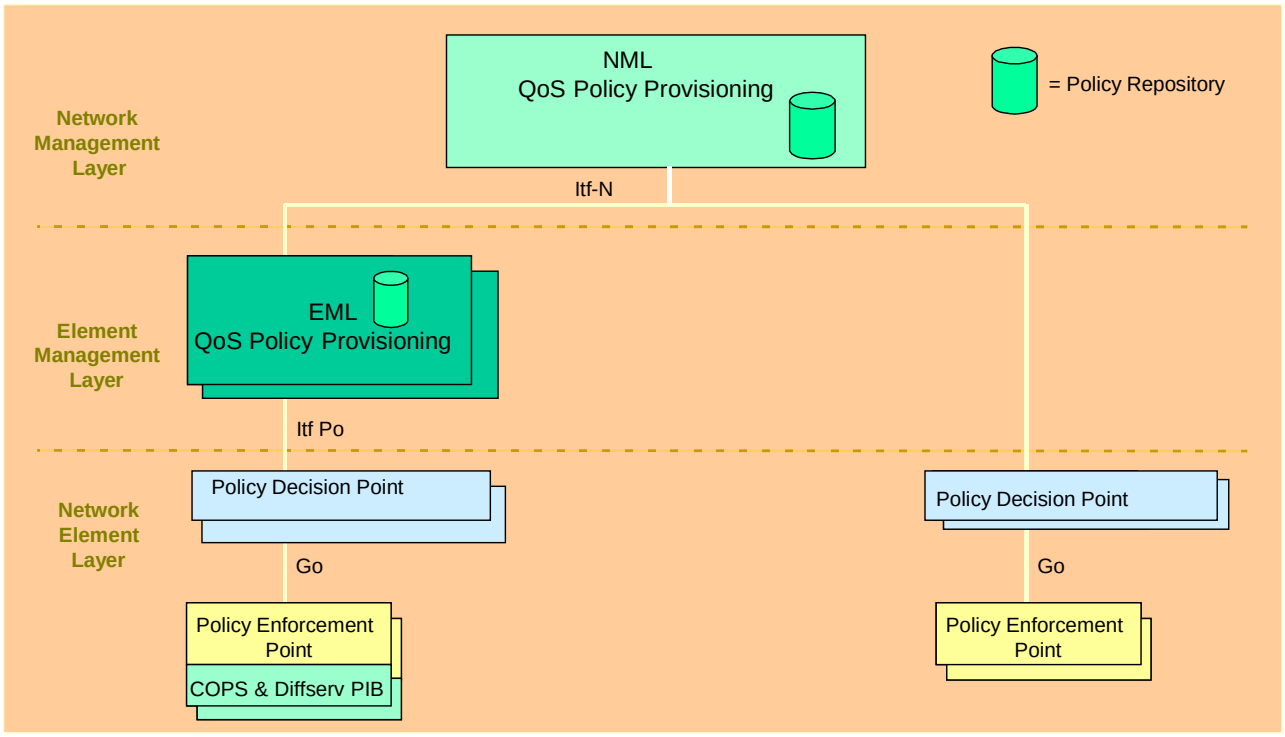


Figure D.2: QoS Provisioning

The architectural components identified in figure D.2 are described in the following clauses.

NOTE: The Policy Repository and the Policy Decision Point can be implemented on the same node.

The Itf N interface is specified in the 32 series.

The Itf Po, between the Policy Repository and the Policy Decision Point is to be defined. The protocols under consideration includes: LDAP, LDUP, SNMP and COPS-PR.

The reference point Go is defined in TS 23.207 (see D.4 QoS Management Reference [22]) and the interface implementing the reference point is defined in TS 29.207 (see D.4 QoS Management Reference [23]).

D.2.2 NML QoS Policy Provisioning

This is a network-level operational support function that serves as the policy administration point for the entire network.

The NML QoS Policy Provisioning provides the following functions:

- Network policy administration user interface
- Master network policy repository for storage of all network policies for all domains
- Policy distribution capability to distribute policy data to the EML Policy servers.
- Global policy conflict detection

The policy repositories will use an LDAP-based directory to store the policy information.

D.2.3 EML QoS Policy Provisioning

This is an element management function that serves as the policy administration point for a network domain. A domain is an area of the network that contains equipment that performs a logically related function. Examples of network domains are: access network, core network and transport network, or supplier specific sub-networks within these networks.

The EML QoS Policy Provisioning provides the following functions:

- An optional EML-level policy administration user interface.
- EML-specific policy repository.
- Policy distribution capability to distribute policy data to the Policy Decision Points.
- Local policy conflict detection

It is envisioned that the optional EML-level policy administration user interface will be required in small networks that do not have a network-level policy provisioning OSS.

Note that EML-specific policy repositories contain policies that apply only to that domain as well as general network policies that apply across domains.

D.2.4 Policy Decision Point

The Policy Decision Point is the point in the network at which policy decisions are made for the Policy Enforcement Points under its scope of control. Whereas the Policy Enforcement Point is a function within a network node, the Policy Decision Point is separate functional entity that may reside within a separate Policy Server, for example, on an application server. The Policy Decision Point will make decisions based on the policy information held within the Policy Repository.

The Policy Decision Point provides the following functions:

- Retrieval of Policy Information from the policy repository
- Evaluates the policy information retrieved and decides what actions needs to taken.
- Distributes policy data to the Policy Enforcement Points. This distribution can either be sent to the PEP by the Policy Decision Point or the Policy Decision Point can wait for the PEP to request the information.
- Translation from QoS policy schema employed by the policy servers to Policy Information Base (PIB) format employed by the Policy Enforcement Points.
- Optional real-time policy decision-making function.
- Local policy conflict detection

The optional real-time policy decision-making function may be required when dynamic policy decisions **must** be made in response to current network conditions.

NOTE: The 3GPP Term Policy Decision Function (PDF) used in 23.207 and 29.207 is equivalent to the IETF Term Policy Decision Point.

TS 23.207 describes the End-to-end Quality of Service (QoS) concept and architecture, and TS 29.207 describes Policy control over Go interface (see D.4 QoS Management Reference [22]) and TS 29.207 (see D.4 QoS Management Reference [23]). If there are any inconsistencies then the definitions in 23.207 and 29.207 take precedence.

D.2.5 Policy Enforcement Point

The Policy Enforcement Point is a function that is part of a Network Element that **must** implement the policies defined by the policy administration system(s).

The Policy Enforcement Point provides the following functions:

- Storage of policy-related data locally.
- Execution of policies as network conditions dictate.
- Support for the Differentiated Services QoS mechanism (diffserv).

On initialization, the Policy Enforcement Point will contact its parent Policy Decision Point and request download of any policy data that it requires for operation. Note that information such as the address of the parent Policy Decision Point function **must** be provisioned in the Policy Enforcement Point MIB as part of normal network provisioning.

TS 23.207 describes the End-to-end Quality of Service (QoS) concept and architecture, and TS 29.207 describes Policy control over Go interface (see D.4 QoS Management Reference [22]) and TS 29.207 (see D.4 QoS Management Reference [23]). If there are any inconsistencies then the definitions in 23.207 and 29.207 take precedence.

D.3 QoS Monitoring

D.3.0 Introduction

QoS Monitoring in 3GPP systems consists of collecting/processing performance statistics, usage data and QoS related faults. In order to obtain end-to-end quality of service monitoring, the Network Elements, the Element Management Layer and Network Management Layer **must** all be involved with the QoS Monitoring process. Alarm and performance collection is done at the Network Element layer and alarm/performance aggregation, report generation, and analysis is done at the Element Management and Network Management layers.

The following functions summarize the QoS Monitoring process:

- Manage QoS fault conditions received from Network Elements.
- Retrieve QoS Performance data from Network Elements.
- Collect and process usage data.
- Generate QoS Reports – trend analysis of key QoS parameters.
- Audit/Analyse collected QoS parameters against expected values.

References that apply to QoS Monitoring and the following clauses are listed in clause D.4.2.

D.3.1 QoS Monitoring Conceptual Architecture

The architecture of a QoS Monitoring system is shown in figure D.3.

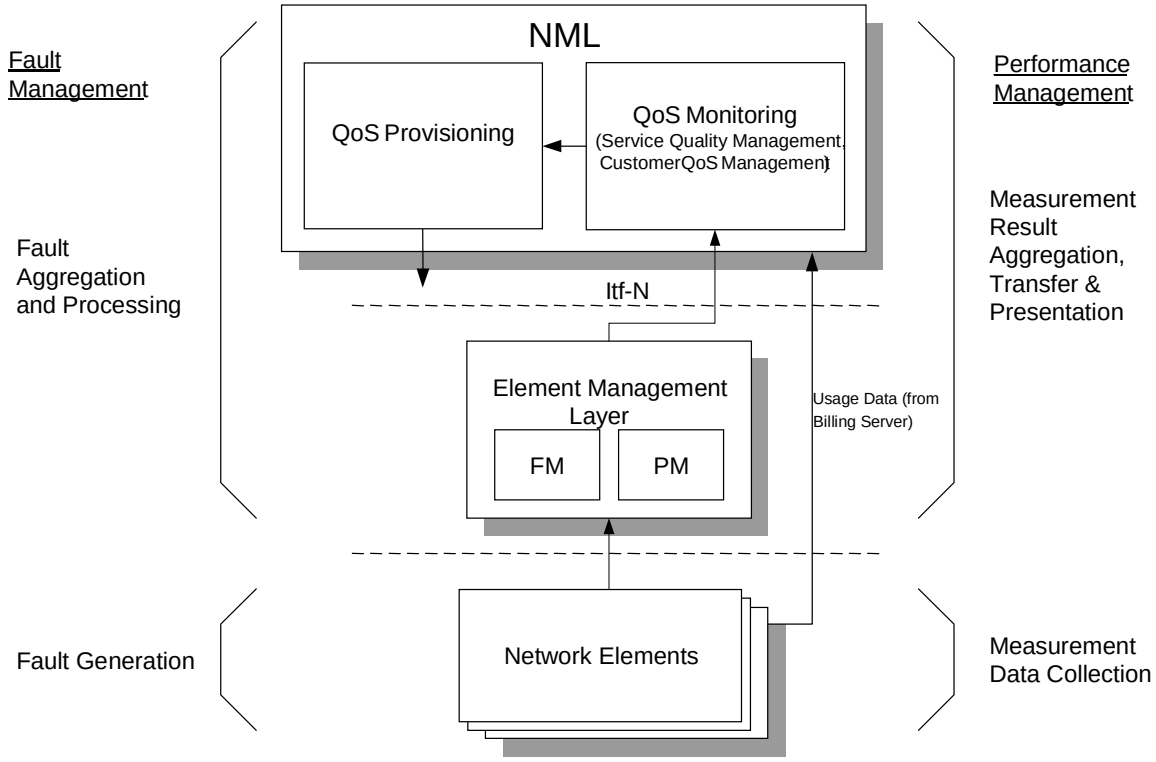


Figure D.3: QoS Monitoring

The architectural components identified in figure D.3 are described in the following clauses.

D.3.2 Network Element

The Network Element component is responsible for collecting performance measurements, usage data and generating alarms. The Network Element component can contain the Policy Enforcement Point or the Policy Decision Point functions.

The Network Element component provides the following functions:

- Collect performance data according to the definition of the measurements and to return results to the EML.
- Collect usage data and forward the data to mediation
- Perform the following fault management functions: Fault detection, Generation of alarms, Clearing of alarms, Alarm forwarding and filtering, Storage and retrieval of alarms in/from the NE, Fault recovery, Configuration of alarms.

D.3.3 Element Management Layer

The Element Management Layer is responsible for aggregating and transferring the collected performance measurements and generated alarms/events.

The Element Management Layer provides the following functions:

Performance Management

- Measurement data collection
  - Measurement types. Corresponds to the measurements as defined in TS 52.402 [24], TS 32.405 [26], TS 32.406 [27], TS 32.407 [28], TS 32.408 [29] and TS 32.409 [30] (see clause D.4 of the present document on QoS Management Reference),
    i.e. measurement types specified in the present document, defined by other standards bodies, or manufacturer defined measurement types;
  - Measured network resources. The resource(s) to which the measurement types shall be applied have to be specified
  - Measurement recording, consisting of periods of time at which the NE is collecting (that is, making available in the NE) measurement data.
- Measurement reporting
  - Measurement Report File Format Definition
  - The measurement related information to be reported has to be specified as part of the measurement. The frequency at which scheduled result reports shall be generated has to be defined.
- Measurement result transfer
  - Measurement results can be transferred from the NE to the EM according to the measurement parameters, and/or they are stored locally in the NE and can be retrieved when required;
  - Measurement results can be stored in the network (NEs or EM) for retrieval by the NM when required.

Fault Management

- Management of alarm event reports
  - Mapping of alarm and related state change event reports
  - Real-time forwarding of event reports
  - Alarm clearing
- Retrieval of alarm information
  - Retrieval of current alarm information on NM request
  - Logging and retrieval of alarm history information on NM request

D.3.4 Network Management Layer

From a QoS Monitoring perspective, the NML is responsible for the collection and processing of performance, fault, and usage data.

The NML QoS Monitoring layer provides the following functions:

- **Service Quality Management** – responsible for the overall quality of a service as it interacts with other functional areas to access monitored information, process that information to determine quality metrics, and initiate corrective action when quality level is considered unsatisfactory. Inputs to SQM include both performance and fault data.

- **Customer QoS Management** – includes monitoring, managing, and reporting the Quality of Service customers receive against what has been promised to the customer in Service Level Agreements and any other service related documents. Inputs to CQM include data from SQM and usage data.

D.4 QoS Management References

D.4.1 Policy Based QoS Provisioning References

The following documents apply to policy-based QoS provisioning:

[1] IETF RFC 3060: "Policy Core Information Model – Version 1 Specification", Moore et al., February 2001.
http://www.ietf.org/rfc/rfc3060.txt

[2] IETF RFC 2251: "Lightweight Directory Access Protocol (v3)", M. Wahl, T. Howes, S. Kille, December 1997. http://www.ietf.org/rfc/rfc2251.txt

[3] IETF RFC 2940: "Definitions of Managed Objects for Common Open Policy Service (COPS) Protocol Clients" ,. A. Smith, D. Partain, J. Seligson. October 2000.
http://www.ietf.org/rfc/rfc2940.txt

[4] IETF RFC 3084: "COPS Usage for Policy Provisioning (COPS-PR)"; K. Chan, J. Seligson, D. Durham, S. Gai, K. McCloghrie, S. Herzog, F. Reichmeyer, R. Yavatkar, A. Smith. March 2001.
http://www.ietf.org/rfc/rfc3084.txt

[5] IETF RFC 2748: "The COPS (Common Open Policy Service) Protocol", J. Boyle, R.Cohen, D. Durham, S. Herzog, R. Rajan, A. Sastry. January 2000, http://www.ietf.org/rfc/rfc2748.txt

[6] IETF RFC 2753: "A Framework for Policy-based Admission Control", R. Yavatkar, D. Pendarakis, R. Guerin. January 2000. http://www.ietf.org/rfc/rfc2753.txt

D.4.2 Policy Based QoS Monitoring References

The following documents apply to QoS monitoring:

[7] 3GPP TS 32.101: " Telecommunication management; Principles and high-level requirements".

[8] 3GPP TS 32.102: " Telecommunication management; Architecture".

[9] 3GPP TS 32.401: "Telecommunication management; Performance Management (PM); Concept and requirements".

[10] 3GPP TS 32.200: "Telecommunication management; Charging management; Charging principles".

[11] 3GPP TS 32.205: "Telecommunications management; Charging management; 3G charging data description for the CS domain".

[12] 3GPP TS 32.215: "Telecommunication management; Charging management; Charging data description for the Packet Switched (PS) domain".

[13] 3GPP TS 32.600: "Telecommunication management; Configuration Management (CM); Concepts and high-level requirements ".

[14] 3GPP TS 32.111-1: "Telecommunication management; Fault Management; Part 1: 3G fault management requirements".

[15] IETF RFC 959: "File Transfer Protocol", J. Postel, J.K. Reynolds. Oct-01-1985. http://www.ietf.org/rfc/rfc0959.txt?number=959

[16] IETF RFC 1901: "Simple Network Management Protocol, v2", J.Case, K. McCloghrie, M. Rose, S. Waldbusser. January 1996. http://www.ietf.org/rfc/rfc1901.txt?number=1901

[17] IETF RFC 2573: "SNMP Applications", D. Levi, P. Meyer, B. Stewart. April 1999. http://www.ietf.org/rfc/rfc2573.txt?number=2573

[18] IETF RFC 1907: "Management Information Base for Version 2 of the Simple Network Management Protocol (SNMPv2)", SNMPv2 Working Group, J. Case, K.McCloghrie, M. Rose, S. Waldbusser. January 1996. http://www.ietf.org/rfc/rfc1907.txt?number=1907

[19] TelemanagementForum (TMF) Telecom Operations Map (TOM), GB910, Approved Version 2.1, March 2000. http://www.tmforum.org/

[20] TelemanagementForum (TMF) TOM Application Note, Mobile Services: Performance Management and Mobile Network Fraud and Roaming Agreement Management, GB910B, Public Evaluation Version 1.1, September 2000. http://www.tmforum.org/

[21] TeleManagement Forum (TMF) NGOSS specifications http://www.tmforum.org/

[22] 3GPP TS 23.207: "End to End Quality of Service QoS Concept and Architecture".

[23] 3GPP TS 29.207: "Policy Control over Go interface".

[24] 3GPP TS 52.402: "Telecommunication management; Performance Management (PM); Performance measurements - GSM".

[25] Void.

[26] 3GPP TS 32.405: "Telecommunication management; Performance Management (PM); Performance measurements - Universal Terrestrial Radio Access Network (UTRAN)".

[27] 3GPP TS 32.406: "Telecommunication management; Performance Management (PM); Performance measurements - Core Network (CN) Packet Switched (PS) domain".

[28] 3GPP TS 32.407: "Telecommunication management; Performance Management (PM); Performance measurements - Core Network (CN) Circuit Switched (CS) domain".

[29] 3GPP TS 32.408: "Telecommunication management; Performance Management (PM); Performance measurements - Teleservice".

[30] 3GPP TS 32.409: "Telecommunication management; Performance Management (PM); Performance measurements - IP Multimedia Subsystem (IMS)".

Annex E (normative): Type 2 protocols and information model for use in Type 4a management interface

The 3GPP management detailed specification has defined protocols and information model (network resource model) for use across Itf-N, i.e. the Type 2 management interface. Some, not all, of these protocols and network resource model are applicable for use across the Itf-P2P, i.e. theType 4a management interface.

The following lists identify the Itf-N protocols and information model relevant for use across Itf-P2P. When certain part of a specific Interface IRP specification (e.g. a particular operation) is not applicable for Itf-P2P, that certain part shall be identified as Exception here.

- List of Interface IRP :
  - [Names of Interface IRP, with possible Exception (see above), are included here. These are to be determined.]
- List of NRM IRP :
  - [Names of NRM IRP included here. The names are to be determined.]

A particular NRM IRP may have defined IOCs that are visible across the Itf-P2P but not visible across Itf-N. In such case, a note “This IOC is visible across Itf-P2P only.” should be part of the subject IOC description.

The standard does not specify which NRM IRP or which IOCs would be invisible across Itf-P2P. That “invisibility” is determined by the two involved peer DMs and is outside the scope of standardization.

At present, the standard does not expect the need to define NRM IRP(s) that are exclusively used by Itf-P2P. In the possible event that the need is required, the standard will specify a convention how to document those NRM IRP(s).

Annex F (informative): Change history

Change history								
Date	**TSG #**	**TSG Doc.**	**CR**	**Rev**	**Subject/Comment**	**Cat**	**Old**	**New**
Mar 2006	SA_31	SP-060100	0027	--	Inclusion of Service Level Tracing Management	B	6.2.0	7.0.0
Mar 2006	SA_31	SP-060099	0029	--	Extension/Generalization of the IRP definition and concept	C	6.2.0	7.0.0
Jun 2006	SA_32	SP-060260	0030	--	Update an obsolete reference related to the Rel-7 withdrawn 32.403	F	7.0.0	7.1.0
Sep 2006	SA_33	SP-060547	0031	--	Add the Domain Manager and its Peer-to-Peer Interface (Itf-P2P) to the Telecom Management Architecture (OAM7-NIM-COOP)	C	7.1.0	7.2.0
Dec 2006	SA_34	SP-060721	0032	--	Add SOAP as an allowed technology for solution sets	B	7.2.0	7.3.0
Dec 2006	SA_34	SP-060721	0033	--	Improve structure and consistency of the definitions related to the IRP concept.	F	7.2.0	7.3.0
Mar 2007	--	--	--	--	Updated the title of Reference [21] ITU-T, added GSM logo	--	7.3.0	7.3.1
Jun 2007	SA_36	SP-070309	0034	--	Identify the Interface IRPs and NRM IRPs which are applicable for Itf-P2P	B	7.3.1	8.0.0
Dec 2007	SP-38	SP-070731	0036	--	Discontinuation of CMIP Solution Sets in Release 7	A	8.0.0	8.1.0
Jun 2008	SP-40	SP-080	0037	--	Remove statement about the Release 7 preferred technologies	F	8.1.0	8.2.0
Sep 2008	SP-41	SP-080465	0038	--	Update of PLMN management processes, relation to IRPs	F	8.2.0	8.3.0
Dec 2008	SP-42	SP-080846	0039	--	Update of PLMN management processes (eTOM supersedes TOM)	F	8.3.0	8.4.0
Sep 2009	SP-45	SP-090627	0040	--	Introduce Service Oriented Architecture (SOA) in the context of Integration Reference Point (IRP)	B	8.4.0	9.0.0
Sep 2009	SP-45	SP-090627	0041	--	Add SOA-based representation of the 3GPP Management Reference Model	B	8.4.0	9.0.0
Mar 2010	SP-47	SP-100035	0042	-	Add missing features and descriptions of Service Oriented Architecture (SOA) in the context of Integration Reference Point (IRP)	B	9.0.0	9.1.0
Mar 2010	SP-47	SP-100035	0044	-	Correction of 3GPP management application layer protocols	F	9.0.0	9.1.0
Mar 2010	SP-47	SP-100035	0045	-	Addition of SOA supporting SS Definitions	B	9.0.0	9.1.0
Sep 2010	SP-49	SP-100489	0046	-	Clarify terms used in IRP framework and architecture	F	9.1.0	10.0.0
Dec 2011	SP-54	SP-110707	0047	-	Recommend NETCONF as a member of Management application layer protocols	B	10.0.0	11.0.0
Dec 2012	SP-58	SP-120799	0048	1	R11 CR 32.101 on Enhancements for Converged Management	B	11.0.0	11.1.0
June 2014	SP-64	SP-140359	0054	-	remove the feature support statements	F	11.1.0	11.2.0
		SP-140345	0055	2	Include the RPT in the Management Reference Model	B		
Sep-2014	SP-65	SP-140571	0057	-	Removal of the Network Management Layer Service (NMLS) in the Management Reference Model	F	11.2.0	11.3.0
			0056	-	Include the Network Management Layer Service (NMLS) in the Management Reference Model	B	11.3.0	12.0.0
Jan-2016					Update to Rel-13 (MCC)		12.0.0	13.0.0

Change history							
Date	**Meeting**	**TDoc**	**CR**	**Rev**	**Cat**	**Subject/Comment**	**New version**
2017-03	SA#75	SP-170140	0065	2	C	Add management entities	14.0.0
2017-09	SA#77	SP-170655	0067	-	C	Addition of management functions and entities	15.0.0
2017-09	SA#77	SP-170655	0068	1	F	Replacement of 3G term	15.0.0
2020-07	SA#88-e	SP-200494	0070	1	B	Introduction of QMC	16.0.0
2022-03	-	-	-	-	-	Update to Rel-17 version (MCC)	**17.0.0**

History

Document history		
V17.0.0	April 2022	Publication