Technical Specification Group Services and System Aspects
Meeting #12, Stockholm, Sweden, 18-21 June 2001

TSGS#12(01)0231

Source: **SA5**

Title: **Rel4 CRs to 3G Telecom Management principles and high level requirements (32.101)**

Document for: **Approval**

Agenda Item: **7.5.3**

Doc-1st-Level	Doc-2nd-Level	Spec	CR	Rev	Phase	Subject	Cat	Version-Current	Version-New	Workitem
SP-010231	S5-010319	32.101	008		Rel4	**Scope update for Rel4**	F	4.0.1	4.1.0	OAM-AR
SP-010231	S5-010370	32.101	009		Rel4	**Updates and Corrections for Rel4**	F	4.0.1	4.1.0	OAM-AR
SP-010231	S5-010371	32.101	010		Rel4	**Alignment with TMF GB910 and associated Editorial improvements**	F	4.0.1	4.1.0	OAM-AR
SP-010231	S5-010372	32.101	011		Rel4	**Update and re-organisation of Clause 8 (Functional Architecture)**	F	4.0.1	4.1.0	OAM-AR
SP-010231	S5-010373	32.101	012		Rel4	**Introduce Subscription Management**	B	4.0.1	4.1.0	OAM-AR
SP-010231	S5-010396	32.101	013		Rel4	**Introduction of QoS Management Annex**	B	4.0.1	4.1.0	OAM-AR
SP-010231	S5-010397	32.101	014		Rel4	**Update the definition of IRP terminology**	F	4.0.1	4.1.0	OAM-AR

3GPP TSG-SA5 (Telecom Management) **S5-010319**
Meeting #20, Brighton, UK, 28 May – June 1 2001 **S5A010101**

CR-Form-v3

CHANGE REQUEST

⌘ **32.101** **CR** **008** ⌘ rev **-** ⌘ Current version: **4.0.1** ⌘

*For **HELP** on using this form, see bottom of this page or look at the pop-up text over the ⌘ symbols.*

Proposed change affects: ⌘ (U)SIM ☐ ME/UE ☐ Radio Access Network **X** Core Network X

Title:	⌘	Scope update for Rel4
Source:	⌘	SA5
Work item code:	⌘	OAM-AR
Date:	⌘	01/06/2001
Category:	⌘	**F**
Release:	⌘	Rel4

Use one of the following categories:
- ***F*** *(essential correction)*
- ***A*** *(corresponds to a correction in an earlier release)*
- ***B*** *(Addition of feature),*
- ***C*** *(Functional modification of feature)*
- ***D*** *(Editorial modification)*

Detailed explanations of the above categories can be found in 3GPP TR 21.900.

Use one of the following releases:

2	*(GSM Phase 2)*
R96	*(Release 1996)*
R97	*(Release 1997)*
R98	*(Release 1998)*
R99	*(Release 1999)*
REL-4	*(Release 4)*
REL-5	*(Release 5)*

Reason for change:	⌘	The scope of 32.101 requirements is unclear in the current document.
Summary of change:	⌘	Addition of two new paragraphs to the Scope section. Addition of Reference to 3G TR 21.801 (Drafting Rules). Correction to clause 4.1.1 introduction and Title. Re-word to last paragraph of clause 4.2
Consequences if not approved:	⌘	The scope of 32.101 requirements may be misinterpreted.

Clauses affected:	⌘	1, 2, 4.1.1, 4.2		
Other specs affected:	⌘	☐ Other core specifications ☐ Test specifications ☐ O&M Specifications	⌘	
Other comments:	⌘			

1 Scope

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

In particular, the present document identifies the requirements for:

- the upper level of a UMTS Management System;
- the reference model, showing the elements the UMTS Management System interacts with;
- the network operator processes needed to run, operate and maintain a UMTS network;
- the functional architecture of the UMTS Management System;
- the principles to be applied to UMTS Management Interfaces;
- the methodology to be followed in further steps of the UMTS Management Specifications.

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

The present document does not provide physical architectures of the UMTS Management System. These aspects are defined and discussed in more detail in 3GPP TS 32.102 [101].

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

~~This document is applicable to all further 3GPP specifications regarding the Network Management of UMTS.~~

2 References

[104] 3GPP TR 21.801 v4.0.0 “Specification Drafting Rules”.

4 General

4.1 UMTS

4.1.1 Basic objectives for UMTS management~~Requirements~~

The requirements and decomposition of Telecom Management for UMTS do not differ radically from that of 2G systems. The following ~~requirements~~ basic objectives to be supported by the UMTS 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 UMTS management.
- to provide the communication between UMTS Network Elements (NEs) and UMTS Operations Systems (OS) or between UMTS OSs themselves via standardised interfaces (e.g. CMIP, CORBA, SNMP, etc.) as appropriate and necessary.
- to minimise the costs of managing a UMTS network such that it is a small component of the overall operating cost.

- to provide UMTS 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 UMTS networks.
- 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 UMTS (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 UMTS and non-UMTS systems.
- 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 a UMTS 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.

4.2 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 UMTS 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 UMTS. However, the UMTS Management needs to explore the incorporation of other concepts (other management paradigms widely accepted and deployed) since:

- UMTS incorporates other technologies to which ITU-T TMN is not applied fully;

- UMTS faces new challenges that ITU-T TMN does not address today;

  The ITU-T standards are mainly concentrated in the element management and network management layers. They have been developed from the bottom up, making it difficult to apply the standards as part of a business case. It is also difficult to have a customer centric focus.

  An example of another management paradigm that will be employed to try and address these difficulties 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.

It can ~~shall~~ be noted that these concerns are applicable to other telecommunication areas as well as to UMTS, it is expected that the eventual evolution of ITU-T TMN will cover this ground. Indeed, most of the above concepts are already being taken into account by ITU-T TMN evolution (protocols and methodologies).

3GPP TSG-SA5 (Telecom Management) **S5-010370**
Meeting #20, Brighton, UK, 28 May – June 1 2001 **S5A010102**

CR-Form-v3

CHANGE REQUEST

⌘ **32.101** **CR** **009** ⌘ rev **-** ⌘ Current version: **4.0.1** ⌘

*For **HELP** on using this form, see bottom of this page or look at the pop-up text over the ⌘ symbols.*

Proposed change affects: ⌘ (U)SIM ☐ ME/UE ☐ Radio Access Network **X** Core Network X

Title:	⌘	Updates and Corrections for Rel4
Source:	⌘	SA5
Work item code:	⌘	OAM-AR
Date:	⌘	01/06/2001
Category:	⌘	**F**
Release:	⌘	Rel4

Use one of the following categories:
- ***F*** *(essential correction)*
- ***A*** *(corresponds to a correction in an earlier release)*
- ***B*** *(Addition of feature),*
- ***C*** *(Functional modification of feature)*
- ***D*** *(Editorial modification)*

Detailed explanations of the above categories can be found in 3GPP TR 21.900.

Use one of the following releases:

2	*(GSM Phase 2)*
R96	*(Release 1996)*
R97	*(Release 1997)*
R98	*(Release 1998)*
R99	*(Release 1999)*
REL-4	*(Release 4)*
REL-5	*(Release 5)*

Reason for change:	⌘	Parts of 32.101 have become outdated, redundant or inaccurate due to evolution of other SA5 specifications.
Summary of change:	⌘	1. Clause 9 is redundant and is deleted; also its reference from the Scope Clause (1) is removed. 2. Two existing definitions are separated as standalone definitions in Definitions Clause (3). 3. Changes to level and ordering of existing sub clauses 5.1 – 5.10. 4. Title change to 5.5 and extra bullet added to bullet list of 5.5. 5. CMIP, CORBA and SNMP comparison lists of 5.8 deleted.
Consequences if not approved:	⌘	Parts of 32.101 will be redundant and outdated.

Clauses affected:	⌘	1, 9, 3, 5
Other specs affected:	⌘	☐ Other core specifications ⌘ ☐ Test specifications ☐ O&M Specifications
Other comments:	⌘	

1 Scope

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

In particular, the present document identifies the requirements for:

- the upper level of a UMTS Management System;
- the reference model, showing the elements the UMTS Management System interacts with;
- the network operator processes needed to run, operate and maintain a UMTS network;
- the functional architecture of the UMTS Management System;
- the principles to be applied to UMTS Management Interfaces;
- ~~the methodology to be followed in further steps of the UMTS Management Specifications.~~

3 Definitions and abbreviations

3.1 Definitions

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

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

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.

~~**Sub-Network Management Functions:** that are 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).~~

Enterprise Systems: those 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).

IRP Information Model: An IRP Information Model consists of an IRP Information Service and a Network Resource Model (see below for definitions of IRP Information Service and Network Resource Model).

IRP Information Service: An IRP Information Service describes the information flow and support objects for a certain functional area, e.g. the alarm information service in the fault management area. As an example of support objects, for the Alarm IRP there is the alarm record and alarm list.

IRP Solution Set: An IRP Solution Set is a mapping of the IRP Information Service to one of several technologies (CORBA/IDL, SNMP/SMI, CMIP/GDMO, etc.). An IRP Information Service can be mapped to several different IRP Solution Sets. Different technology selections may be done for different IRPs.

Management Infrastructure: The collection of systems (computers and telecommunications) a UMTS Organisation has in order to manage UMTS.

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.

Network Resource Model (NRM): A protocol independent model describing managed objects representing network resources, e.g. an RNC or NodeB.

Sub-Network Management Functions: that are 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).

UMTS Organisation: A legal entity that is involved in the provisioning of UMTS.

5 Architectural framework

5.1 UMTS Management Reference Model and Interfaces

5.1.1 Overview

Figure 1 illustrates the UMTS Management Reference Model. It shows the UMTS Operation System interfacing with other systems.

The present document (and the rest of the 3GPP UMTS Management detailed specifications) addresses the UMTS 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 UMTS Operations System may interface to. The rest of the 3GPP specifications regarding UMTS 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 UMTS. However, it is the intention to identify and define what will be needed from the perspective of UMTS management.

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

1) between the NEs and the Operations System of a single UMTS Organisation:
    a) network element to element management level;
    b) element management to network management level.
2) between the Operations System and the Enterprise Systems of a single UMTS Organisation;
3) between Operations Systems of different UMTS Organisations;
4) within the Operations System of a single UMTS Organisation.

The present document focuses on management interfaces of type 1 from the above list, while interfaces of types 2 & 3 will be identified in the present document. Detailed specification of these interfaces is For Further Study (FFS). Interfaces of type 4 are beyond the scope of standardisation.

NOTE: Both TeleManagement Forum and ITU-T are carrying out work with interfaces of type 3.

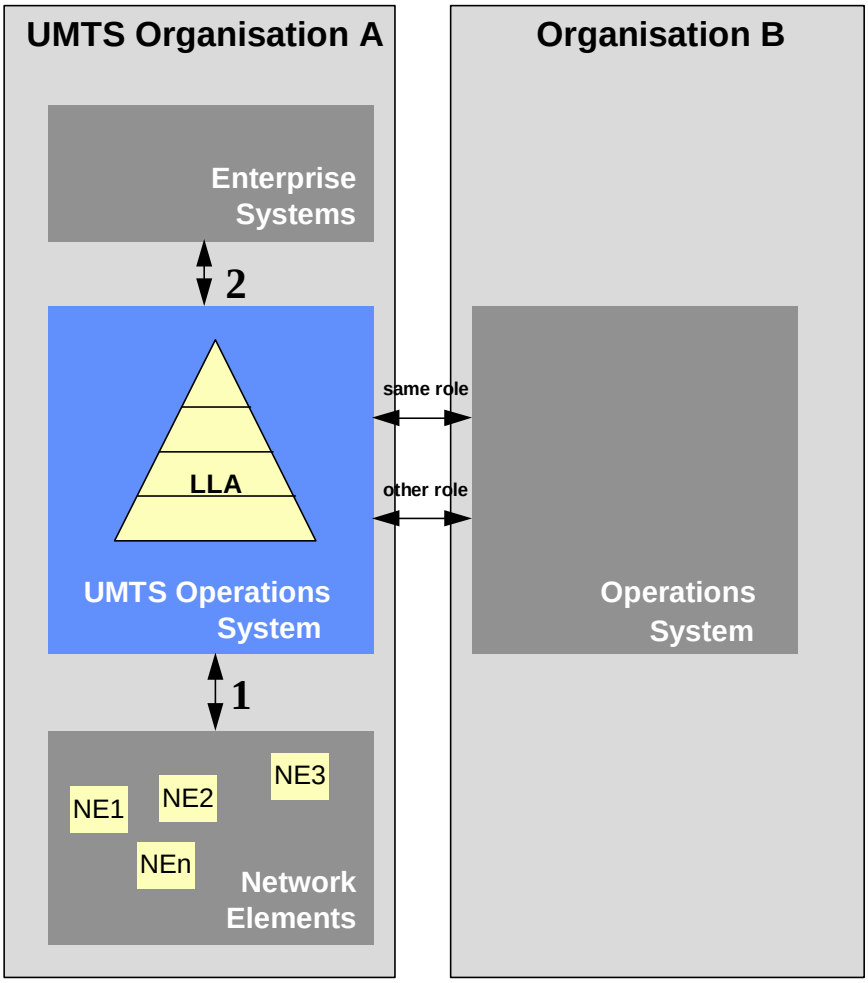


Figure 1: UMTS Management System Interactions

5.1.2 Interfaces to NEs (Type 1)

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

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

It is assumed that this will not fully cover the O&M functionality of all NE types in UMTS 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 rational 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 rational 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).

The approach for NE Management Interfaces will be to concentrate on protocol independent information models, allowing a mapping to several protocol suites. The rational is:

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

However, it is the intention to a least recommend one mapping for each interface.

5.1.3~~5.2~~ Interfaces to Enterprise Systems (Type 2)

It is the approach to define a UMTS Management that fully fits into the enterprise processes needs of the UMTS 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 UMTS Operations Systems are defined, to allow for easy interconnection and functional support.

~~5.3 Interfaces to NEs (Type 1)~~

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

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

~~It is assumed that this will not fully cover the O&M functionality of all NE types in UMTS 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 rational 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 rational 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).~~

~~The approach for NE Management Interfaces will be to concentrate on protocol independent information models, allowing a mapping to several protocol suites. The rational is:~~

- ~~due to the convergence of Information and Telecommunication technologies in UMTS, it is required to work on a more open approach (acknowledging the market status and foreseen evolutions);~~
- ~~the life cycle of information flows is 10 to 20 years, while that of protocols is 5 to 10 years;~~
- ~~developments in automatic conversion from information models to various protocols/technologies will allow a more pragmatic and open approach (e.g. UML to GDMO, UML to IDL).~~

~~However, it is the intention to a least recommend one mapping for each interface.~~

5.1.4~~5.4~~ Interfaces to other Operations Systems (Type 3)

UMTS Management considers integrally the interaction between the Operations Systems of other legal entities for the purpose of providing UMTS services.

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

1) to other UMTS Operations Systems (i.e. other from other UMTS operators);
2) to other Operations Systems (i.e. to non-UMTS operators).

The first type deals with co-operation to provide UMTS services across a number of UMTS 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 a UMTS 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).

5.25 Interface levelsdefinition

5.2.1 Overview

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

1) 1) logical (information model and flows used in the relationship manager-agent, or equivalent);

2) Solution Set (SS) Level

32) application protocol (end-to-end, upper layers protocol running between manager-agent, or equivalent);

43) networking protocol (lower layer protocols carrying the information in/out the manager and agent, or equivalents);

54) physical (mapping of the manager and agent, or equivalents, roles into physical entities).

Figure 2 shows the management interfaces of one part of the UMTS (the Radio Network), by way of illustration of interfaces of types 1a and 1b).

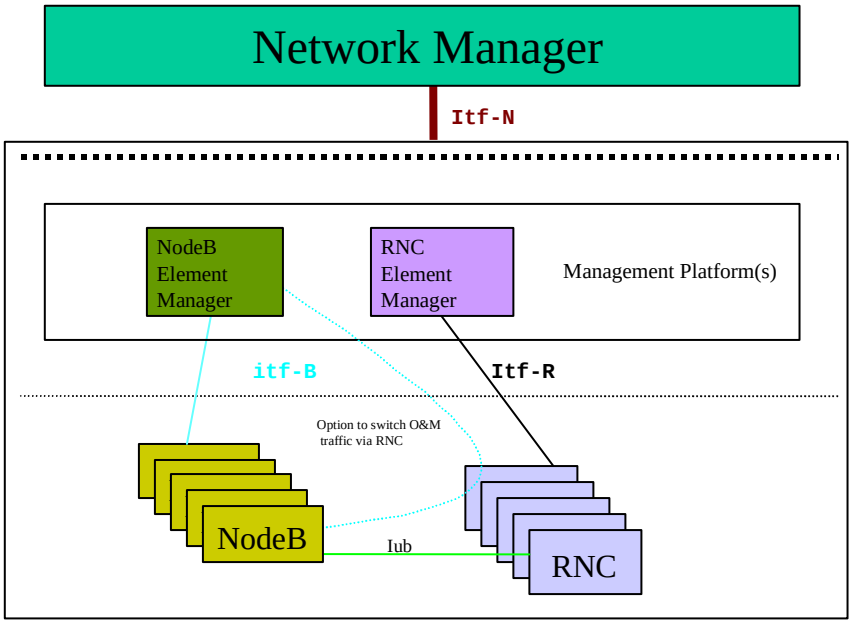


Figure 2: Radio Network Management Interfaces

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 1a).
- Itf-R - between RNC & its Manager (type 1a).
- Itf-N – between Network & Network Manager (type 1b).

5.2.2~~5.6~~ Logical level

This level covers the mutual and conceptual knowledge of entities being connected by a given interface.

For type 1b interfaces (such as Itf-N in Figure 2 above) interactions at this level are fully standardised by 3GPP in terms of protocol independent Network Resource Models (static information definition) and IRP Information Services (information flows) where available. These protocol-independent Network Resource Models and IRP Information Services are hereafter referred to as IRP Information Models (Integration Reference Point Information Models).

5.2.3~~5.7~~ Solution Set (SS) level

For each IRP Information Model at the logical level there will be at least one IRP Solution Set defined. An IRP Solution Set is a mapping of the IRP Information Service to one of several technologies (for a full definition refer to subclause 3.1).

See Annex C for the valid UMTS Management IRP Solution Sets.

5.2.4~~5.8~~ Application 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.

Generally, the Application Protocol Suite used for the interaction between entities across a given interface is optional within the valid UMTS Management Application Protocol Suites (see Annex A for a list of UMTS Management Protocol Suites). However, in the case of interfaces of type 1b (such as Itf-N in figure 2 above) at least one of those protocol suites will be chosen as the standard protocol suite.

~~It is the intention to consider following attributes of each application protocol in making this decision:~~

~~CMIP:~~

- ~~Very flexible;~~
- ~~Powerful information modelling capability, therefore, in turn, complex to implement;~~
- ~~Complex to integrate managers (specifically if CMIP stacks from different vendors are used in the agents and manager(s));~~
- ~~Process hungry;~~
- ~~Heavyweight stack (e.g. prevents it from being implemented on NodeB);~~
- ~~Potential reuse of GSM and ITU-T standards and implementation;~~
- ~~High on Cost Of Goods.~~

~~SNMP:~~

- ~~is well used in other Telecom areas (e.g. ATM management);~~
- ~~has inadequacies for Configuration Management (relatively simple/poor information modelling capability for management MIBs make implementation of complex information models difficult, although not impossible);~~
- ~~supports auto-discovery of elements on the management network via MIB-II;~~
- ~~has lower Cost Of Goods;~~
- ~~more choice of "off the shelf commercial systems and software" (see subclause 7.2 and 3GPP TS 32.102 [101]).~~

~~CORBA IIOP:~~

- ~~very powerful and flexible;~~
- ~~low Cost Of Goods;~~

- not proven in Telecom Management (but gaining acceptance).

5.2.5~~5.9~~ 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 UMTS 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 ~~any~~ 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~~5.10~~ Physical level

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

NOTE: Q-Adapter needs to be interpreted here in a wider sense than in ITU-T Recommendation M.3010 [1], since UMTS will consider other application protocols different to CMIP.

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

5.3~~11~~ Compliance conditions

For a UMTS entity (Management System or NE) to be compliant to a given UMTS Management Interface, all the following conditions shall be satisfied:

- it implements the management functionality following the Information Model and flows specified by the relevant 3GPP UMTS Management Interface Specifications applicable to that interface;
- it provides at least one of the IRP Solution Sets (where available) related to the valid Application Protocols specified by 3GPP UMTS 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;
- 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 UMTS NE and/or UMTS Management System.

~~9 Methodology~~

~~9.1 Documentation~~

~~The methodology followed for the specification of UMTS Management is structured in the following levels and steps:~~

~~9.1.1 UMTS Management Overall Architecture, Functionality/Processes and Principles specification~~

~~The UMTS Management Overall Architecture, Functionality/Processes and Principles are specified in the present document.~~

~~9.2 Tools and Methods~~

~~The tool and method to be used for documenting Interface Specifications will be UML.~~

Annex C (normative): UMTS Management IRP Solution Sets

The valid IRP Solution Sets for the Management of UMTS on the Itf-N interface are:

- ~~CMIP/~~GDMO (CMIP);
- ~~CORBA/~~IDL (IDL).

3GPP TSG-SA5 (Telecom Management) **S5-010371**
Meeting #20, Brighton, UK, 28 May – June 1 2001 **S5A010103**

CR-Form-v3

CHANGE REQUEST

⌘ **32.101** **CR** **010** ⌘ rev **-** ⌘ Current version: **4.0.1** ⌘

*For **HELP** on using this form, see bottom of this page or look at the pop-up text over the ⌘ symbols.*

Proposed change affects: ⌘ (U)SIM ☐ ME/UE ☐ Radio Access Network **X** Core Network X

Title:	⌘	Alignment with TMF GB910 and associated Editorial improvements
Source:	⌘	SA5
Work item code:	⌘	OAM-AR
Date:	⌘	01/06/2001
Category:	⌘	**F**
Release:	⌘	Rel4

Use one of the following categories:
F *(essential correction)*
A *(corresponds to a correction in an earlier release)*
B *(Addition of feature),*
C *(Functional modification of feature)*
D *(Editorial modification)*
Detailed explanations of the above categories can be found in 3GPP TR 21.900.

Use one of the following releases:
2 (GSM Phase 2)
R96 (Release 1996)
R97 (Release 1997)
R98 (Release 1998)
R99 (Release 1999)
REL-4 (Release 4)
REL-5 (Release 5)

Reason for change:	⌘	32.101 uses and references concepts from the TMF Telecom Operations MAP version 1.1. A later version (2.1) is now available and 32.101 should be aligned with this.
Summary of change:	⌘	A new TOM diagram is added which supersedes the previous one, Process descriptions and references are updated according to TMF GB910 Version 2.1 (Telecom Operations Map). As a result of these changes and to improve readability Clauses 6 and 7 are merged and part of Clause 6 is updated and moved to Clause 8 (new Clause 7).
Consequences if not approved:	⌘	Divergence of 3GPP SA5 and TMF specifications.

Clauses affected:	⌘	2, 6, 7 and 8
Other specs affected:	⌘	☐ Other core specifications ⌘ ☐ Test specifications ☐ O&M Specifications
Other comments:	⌘	

2 References

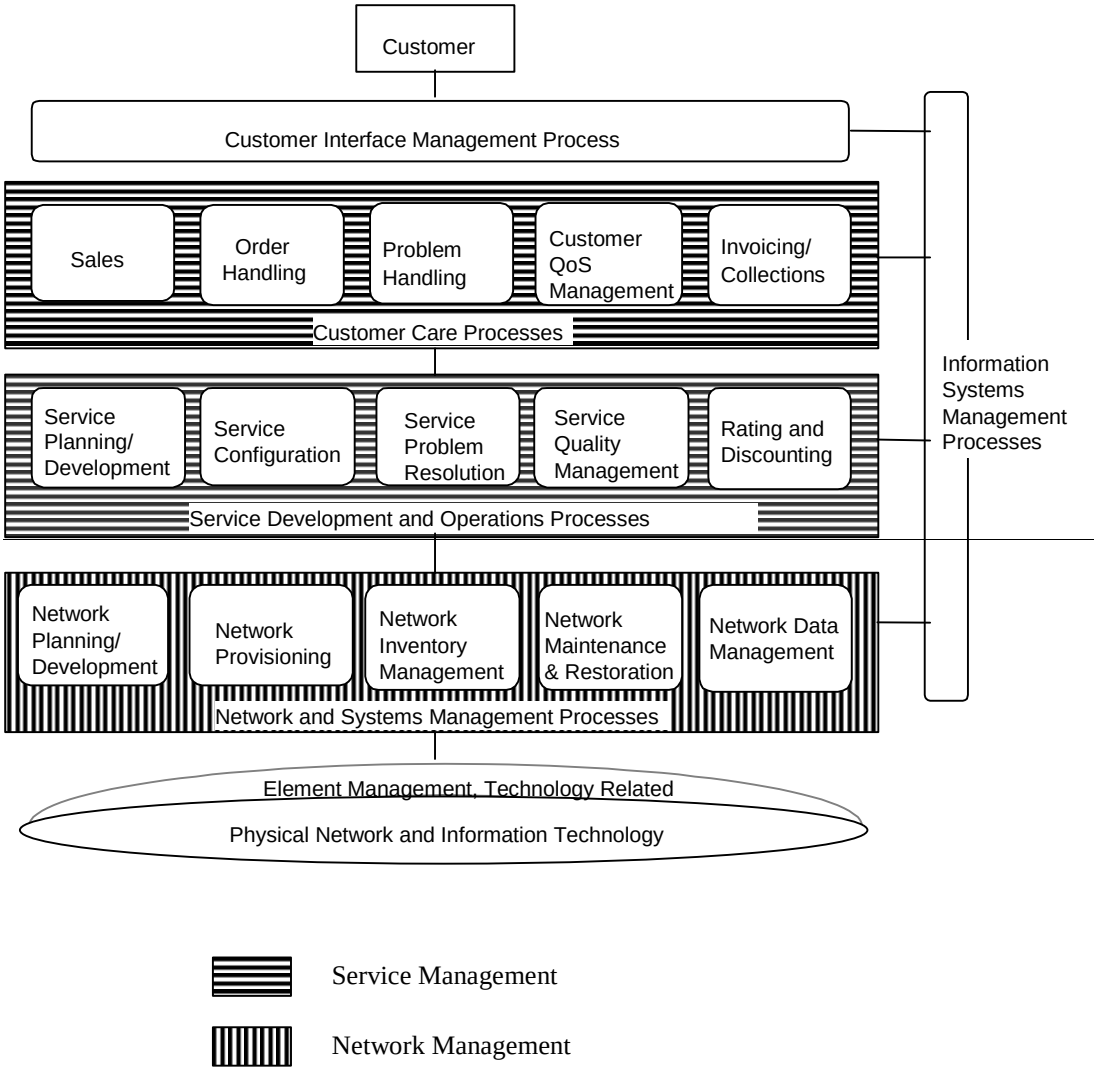
[100] TMF GB910: "Telecom Operations Map"; ~~Evaluation Release~~ Approved Version ~~1~~2.1 March 2000, (May be downloaded from http://www.tmforum.org.) ~~April~~.

6 UMTS Management Processes

6.1 Process decomposition

The present document details the general aspects of an UMTS Management system. It describes primarily the management processes that collectively support Customer Care Service Development & Operations, and Network & Systems Management Processes in an UMTS network.

These management processes are based on the widely accepted Telecom Operations Map from the TeleManagement Forum [100]. The Telecom Operations Map uses the TMN Model as a foundation~~They map onto the Service and Network Management layers~~ as defined in the ITU-T Recommendation M.3010 ~~appendix II~~ [1] ~~as depicted in Figure 3 below.~~



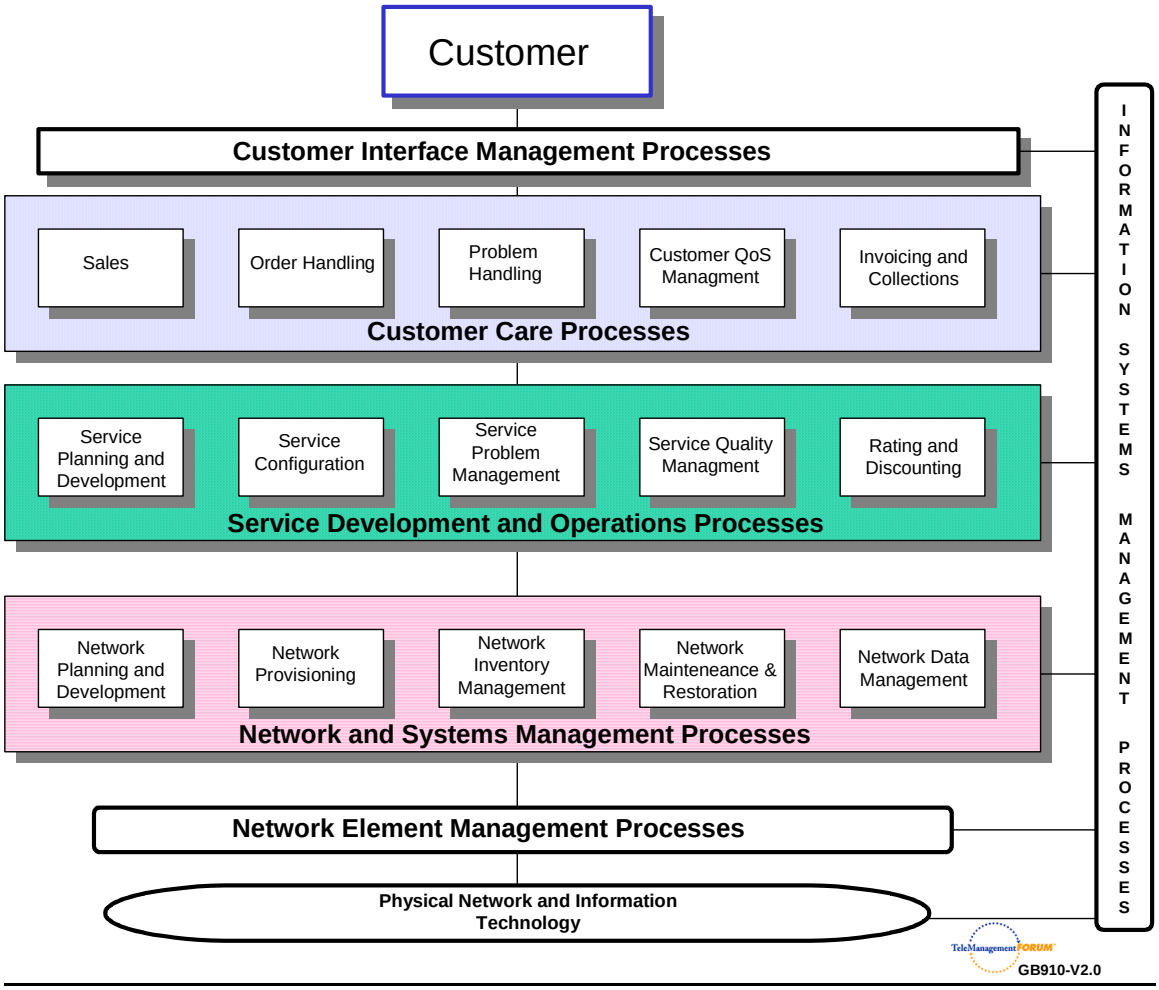


Figure 3: Telecom Operations Map Business Process Model (* imported from [100])
(Service & Network Management shading added in the present document)

The present document details the UMTS Management Functional Architecture. This is done by applying each of the management functions to the UMTS management processes.

The management functions are:

- fault management;
- configuration management (including equipment inventory);
- performance management (including quality of service management);
- roaming management;
- accounting;
- customer profile management;
- service deployment;
- fraud management;
- security management;
- software management.

All UMTS 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 Telecom Operations Map that details the functional architecture for performance management, this will be the approach taken by the present document.~~

~~7 Process decompositions~~

The~~is~~ following clause~~s~~ gives a short description of each of the UMTS management processes introduced in the "TMF Telecom Operations Map" [100]. To see a more detailed description and process spider diagram for each process, refer to "TMF Telecom Operations Map"[100].

6.2 Customer Care Processes

These processes involve direct interaction with a customer to provide, maintain, report on service, and bill for services. The customer is the ultimate buyer of a communications service with many end users in their organization that utilize the Service Provider's services. The Service Provider must interact at many interfaces to support its customer and end users.

6.2.1~~7.1~~ Customer Interface Management

The Customer Interface Management Process may be a distinct process, or may be performed as part of the individual Customer Care Processes on an individual service or cross-service basis. These are the processes of directly interacting with customers and translating customer requests and inquiries into appropriate "events" such as, the creation of an order or trouble ticket or the adjustment of a bill. ~~The Customer Interface Management Process directly interacts with customers and translates customer requests and inquiries into appropriate "events" such as, the creation of an order or trouble ticket or the adjustment of a bill.~~

6.2.2~~7.2~~ Sales

The Sales Process encompasses learning about the needs of each customer, and educating the customer about the communications services that are available to meet those needs.

6.2.3~~7.3~~ Order~~ing~~ Handling

The Order Handling Process includes all the functions of:

- Accepting a customer's order for service, whether directly from the customer, from the Sales process, from the customer's agent (e.g., Outsourcer, another service provider)
- Tracking the progress of the order and updating the customer
- Notifying the customer when the order is complete

~~The Ordering Process includes all the functions of accepting a customer's order for service, tracking the progress of the order, and notifying the customer when the order is complete.~~

6.2.4~~7.4~~ Problem Handling

The Problem Handling Process is responsible to receive service complaints from customers, resolve them to the customer's satisfaction and provide meaningful status on repair or restoration activity.

6.2.5~~7.5~~ Customer QoS Management

This process encompasses monitoring, managing and reporting of UMTS Quality of Service (QoS) as defined in Service Descriptions, Service Level Agreements (SLA), and other service-related documents. ~~This process is concerned with UMTS Quality of Service (QoS) and its measurement, management and reporting.~~

6.2.6~~7.6~~ Invoicing and Collection

This process encompasses sending invoices to customers, processing their payments and performing payment collections. In addition, this process handles customer inquiries about bills, provides billing inquiry status and is responsible for resolving billing problems to the customer's satisfaction.

6.3 Service Development and Operations Processes

These processes are generally "one step removed" from day-to-day direct customer interaction. Focus is on service delivery and management as opposed to the management of the underlying network and information technology. Some of these functions are done on a one-time basis, like designing and developing a new service or feature. Other functions involve service capacity planning, the application of a service design to specific customers or managing service improvement initiatives, and are closely connected with the day-to-day customer experience.

6.3.1~~7.7~~ Service Planning and Development

This process encompasses:

- ~~designing~~Designing technical capability to meet specified market need at desired cost;
- Negotiating joint service arrangements, e.g., SLAs with other providers, Mobile Services Roaming Agreements, Bilateral Agreements etc. Inter-Provider Agreements.
- ~~ensuring~~Ensuring that the service (product) can be properly installed, monitored, controlled, and billed;
- ~~initiating~~Initiating appropriate process and methods modifications, as well as initiating changes to levels of operations personnel and training required;
- ~~initiating~~Initiating any modifications to the underlying network or information systems to support the requirements;
- Assuring that the technical capability works, that the operational support process, procedures, and systems function properly.
- Managing deployment and Controlled Introduction of a new service, feature, enhancement or other change to the service.
- ~~performing pre-service testing that the technical capability works and that the operational support process and systems function properly;~~
- ~~ensuring~~Ensuring that sufficient capacity is available to meet forecasted sales.

6.3.2~~7.8~~ Service Configuration

This process encompasses the installation and/or configuration of service for specific customers, including the installation/configuration of customer premises equipment.

6.3.3~~7.9~~ Service Problem Management~~Resolution~~

This process encompasses reporting on service problems and trouble performance, isolating the root cause of service-affecting and non-service-affecting failures and acting to resolve them. ~~This process encompasses isolating the root cause of service affecting and non-service affecting failures and acting to resolve them.~~ Typically, failures reported to this process affect multiple customers.

6.3.4~~7.10~~ Service Quality Management

This process supports monitoring service or product quality on a service class basis in order to determine:

- ~~whether~~Whether service levels are being met consistently;

- Whether there are any problems with or improvements that can be made for the service or product;

- ~~whether there are any general problems with the service or product;~~

- ~~whether~~Whether the sale and use of the service is tracking to forecasts.

6.3.5~~7.11~~ Rating and Discounting

This process encompasses:

- Applying the correct rating rules to usage data on a customer-by-customer basis, as required for a usage based service ~~applying the correct rating rules to usage data on a customer-by-customer basis, as required;~~

- ~~applying~~Applying any discounts agreed to as part of the Ordering Process;

- ~~applying~~Applying promotional discounts and charges;

- ~~applying~~Applying outage credits;

- Applying rebates or charges due because Service Level Agreements were not met or exceeded respectively; ~~applying rebates due because service level agreements were not met;~~

- Resolving unidentified and zero billed usage cases. ~~resolving unidentified usage.~~

6.4 Network and Systems Management Processes

These processes are responsible for ensuring that the network and information technologies infrastructure supports the end-to-end delivery of the required services.
The job of these processes is to implement the infrastructure required, ensure it runs smoothly, is accessible to services, is maintained and is responsive to the needs, whether directly or indirectly, of services and customers. Network and Systems Management is also the integration layer between the Element Management Layer and the Service Management Layer. Its basic function is to assemble information from the 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 network.

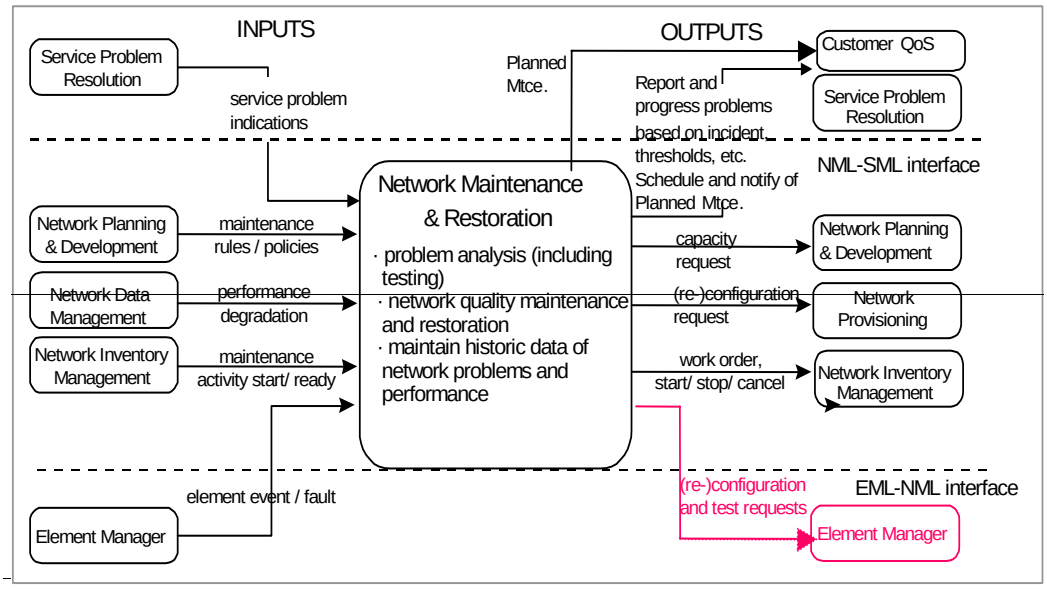
6.4.1~~7.12~~ Network Data Management

This process encompasses the collection of usage data and network and information technology events and data for the purpose of network performance and traffic analysis. This data may also be an input to Billing (Rating and Discounting) processes at the Service Management Layer, depending on the service and its architecture. ~~In general, this process is responsible for the collection of performance/usage data and events for the purpose of network performance, usage and traffic analysis. This data is also an input to the Rating and Discounting process at the Service Management Layer.~~

6.4.2~~7.13~~ Network Maintenance and Restoration

This process encompasses maintaining the operational quality of the network, in accordance with required network performance goals.

~~NOTE: 3GPP have added an additional process flow to this process. For this reason a modified spider diagram for this process is included in Figure 4 below (changes highlighted in red). This change has been submitted to TMF for inclusion in the Telecom Operations Map (TOM), when the changes is incorporated in the TOM the diagram can be removed from the present document.~~



~~NOTE: Red colours in this figure indicate changes to Telecom Operations Map not yet approved by the TMF.~~

~~Figure 4: Network Maintenance and Restoration Process~~

6.4.3~~7.14~~ Network Inventory Management

This process encompasses anything to do with physical network and information technology equipment and the administration of this equipment. ~~This process encompasses anything to do with physical equipment and the administration of this equipment.~~

6.4.4~~7.15~~ Network Provisioning

This process encompasses the configuration of the network, to ensure that network capacity is ready for provisioning and maintenance of services.

6.4.5~~7.16~~ Network Planning and Development

This process encompasses:

- Development and acceptance of network and information technology infrastructure strategies.
- Description of standard network configurations primarily for operational use.
- Definition of rules for networks, e.g., planning, installation, usage recording and maintenance, etc.
- Designing the network capabilities to meet a specified service need at the desired cost, i.e., the introduction of new technologies to support new services, features or enhancements.
- Design, deployment and introduction of new technologies for network and information technology cost reductions or quality improvements.
- Ensuring that the network can be properly installed, monitored and controlled.
- Ensuring that enough network capacity will be available to meet the forecasted demand. Based on the required network capacity, orders are issued to suppliers or other network operators (ONOs) and site preparation and installation orders are issued to Network Inventory Management or a third party network constructor (work orders). A design of the logical network configuration is provided to Network Provisioning.

Supporting cases of un-forecasted demand.

~~This process encompasses development and acceptance of strategy, description of standard network configurations for operational use, definition of rules for network planning, installation and maintenance.~~

7~~8~~ UMTS Management Functional Architecture

7.1~~8.1~~ 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 below.

The present document addresses the Functional Architecture, the Physical Architecture is addressed in 3GPP TS 32.102 [101].

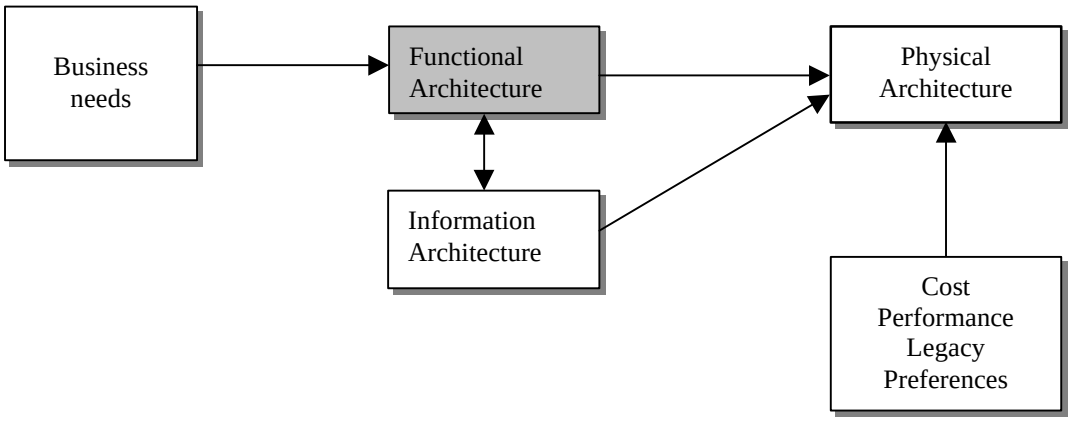


Figure ~~4~~5: Architectural relationship

The present document details the UMTS Management Functional Architecture.

All UMTS 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 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

- User equipment management

3GPP TSG-SA5 (Telecom Management) **S5-010372**
Meeting #20, Brighton, UK, 28 May – June 1 2001 **S5A010104**

CR-Form-v3

CHANGE REQUEST

⌘ **32.101** **CR** **011** ⌘ rev **-** ⌘ Current version: **4.0.1** ⌘

*For **HELP** on using this form, see bottom of this page or look at the pop-up text over the ⌘ symbols.*

Proposed change affects: ⌘ (U)SIM ☐ ME/UE ☐ Radio Access Network **X** Core Network X

Title:	⌘	Update and re-organisation of Clause 8 (Functional Architecture)
Source:	⌘	SA5
Work item code:	⌘	OAM-AR
Date:	⌘	01/06/2001
Category:	⌘	**F**
Release:	⌘	Rel4

Use one of the following categories:
F *(essential correction)*
A *(corresponds to a correction in an earlier release)*
B *(Addition of feature),*
C *(Functional modification of feature)*
D *(Editorial modification)*
Detailed explanations of the above categories can be found in 3GPP TR 21.900.

Use one of the following releases:

2	*(GSM Phase 2)*
R96	*(Release 1996)*
R97	*(Release 1997)*
R98	*(Release 1998)*
R99	*(Release 1999)*
REL-4	*(Release 4)*
REL-5	*(Release 5)*

Reason for change:	⌘	Clause 8 (Functional Architecture) has become outdated due to evolution of existing SA5 and TMF specifications
Summary of change:	⌘	References to SA5 and TMF specifications added, redundant material removed, new material introduced and general editorial improvements made.
Consequences if not approved:	⌘	Incomplete and outdated Functional Architecture in 32.101

Clauses affected:	⌘	2, 8
Other specs affected:	⌘	☐ Other core specifications ⌘ ☐ Test specifications ☐ O&M Specifications
Other comments:	⌘	The correct section and figure numbering of this CR is dependent on the approval of CR32.101-010_S5-010371.

2 References

[53] 3GPP TS 32.104-series: "3G Performance Management Requirements".

[54] 3GPP TS 32.600: "3G Configuration Management Requirements".

[105] TMF GB910B: “TOM 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.)

7.28.2 Performance Management

7.2.1 Overview

An initial view of Performance Management is described in [104]. 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 [104] for further detail.

7.2.2 Standardisation Objectives

During the lifetime of a 3G network, 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 3GPP TS 32.600 [54].

Many of the activities involved in the daily operation and future network planning of a 3G network 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 3G network. 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 this standardisation are:

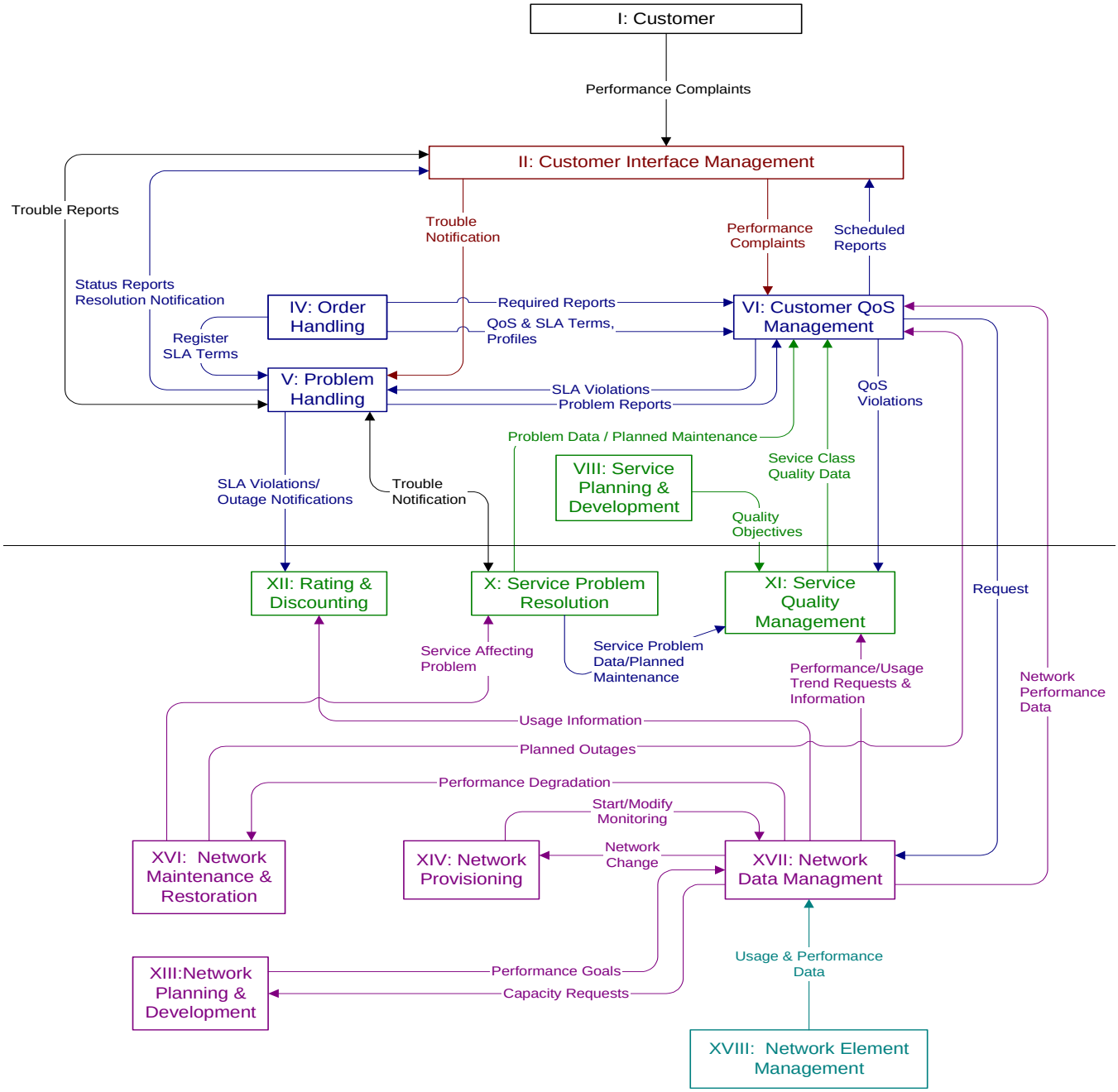
- To provide the descriptions for a standard set of measurements;
- To produce a common description of the management technique for measurement administration and result accumulation; and
- To define a method for the bulk transmission of measurement results across a management interface.

The definition of the standard measurements is intended to result in comparability of measurement data produced in a multi-vendor 3G network, 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 3GPP TS 32.104-series [53].

~~Figure 6 below makes a cut through the Telecom Operations Map from a Performance Management perspective. Although this "cut slice" is quite large it does not contain all and everything related to Performance Management. But it contains all processes and interfaces mainly involved in Performance Management. To make Figure 6 clearer different thickness of lines have been used to illustrate the different importance of the accordingly marked interfaces.~~



~~Figure 6: Information flow to support Performance Management~~

7.38.3 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 traveling in an area supported by another network as the customer receives when in their home service provider's area. Please refer to [104] to see an example implementation with more detail ~~This example describes a unique, for mobile networks, management task. Roaming is a service provided by mobile service providers where customers of a home service provider may use the infrastructure of another, a serving service provider (see Figure 7). The idea is that a customer receives the same service when it roams in another network, as it would receive at home.~~

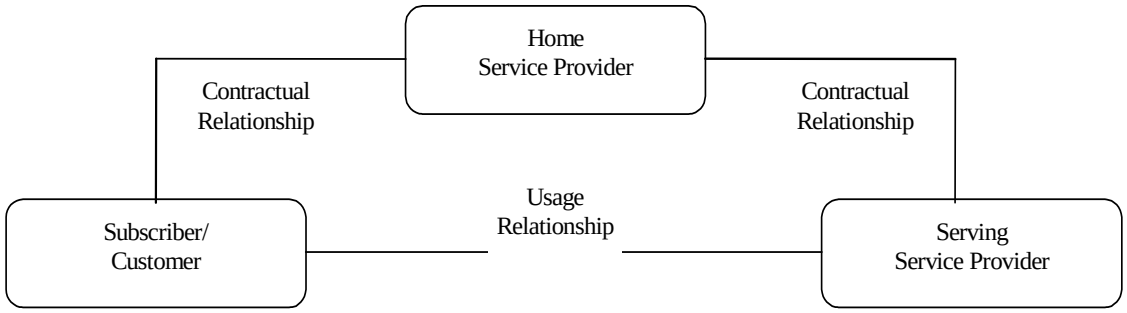


Figure 57: Relationships between Subscriber, Home and Serving Service Provider

~~In order to make this happen, the home service provider and serving service provider need a contractual relationship called a roaming agreement. The roaming agreement can be an ordinary direct agreement between both service providers or it can be established by the means of a clearinghouse.~~

~~In any case the roaming agreement regulates at least the following items:~~

- ~~tariffing and pricing;~~
- ~~signalling and traffic interconnection;~~
- ~~CDR exchange format and exchange schedule;~~
- ~~problem handling; and many others.~~

~~Today's mobile networks have roaming agreements with tens of other networks. With 3rd Generation mobile networks coming, this number is expected to increase to hundreds if not more. All these roaming agreements have an impact on many parts of the network.~~

~~The handling of this complex process requires an excellent understanding of roaming agreement management. To aid this understanding Figure 8 below is provided. All information flows, which are not effected or not changed by roaming agreement management, have been omitted to aim readability.~~

~~NOTE: The information flows shown in Figure 8 are intended to illustrate the flow of management information required to support roaming in 3rd Generation networks.~~

~~The information flow illustrated in Figure 8 is an overlay onto the main information flow of a serving mobile service provider to support it's own subscribers. This overlay information flow of the serving service provider is triggered by the request to establish or update a roaming agreement issued by the customer.~~

~~In this context the home service provider is classified as a customer of a serving service provider (customer in this context does not refer to an individual customer of the home service provider!).~~

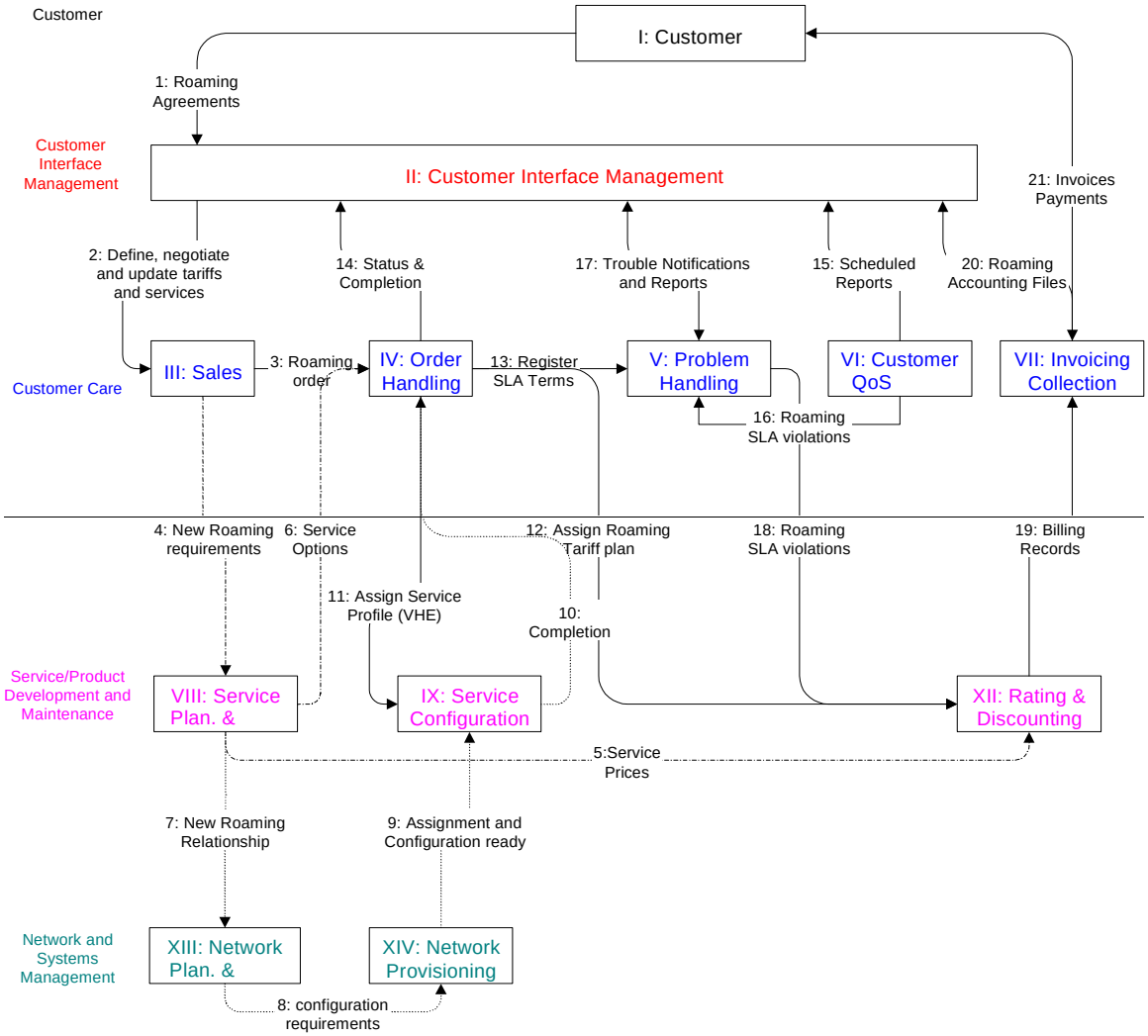
~~The home service provider (customer) would like to offer roaming to the serving service provider to its subscribers.~~

~~The roaming agreement management information flow consists of one major and two optional supporting information flows:~~

- ~~customer care information flow (solid line)~~
  ~~This is the major information flow supporting all contract related activities: negotiating tariffs, negotiating SLAs, trouble handling, roaming accounting file exchange,...~~

- ~~new service facilities information flow (dash-dotted line)~~
  ~~This is an optional supporting flow which takes place if the support of an roaming agreement requires the introduction of new services or a configuration change of existing services.~~

- ~~new network facilities information flow (dashed line)~~
  ~~This is an optional supporting flow which takes place if the support of an roaming agreement requires the introduction of new network facilities or a configuration change of existing network facilities.~~



~~Figure 8: Information flow to support Roaming Management~~

7.4~~8~~.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

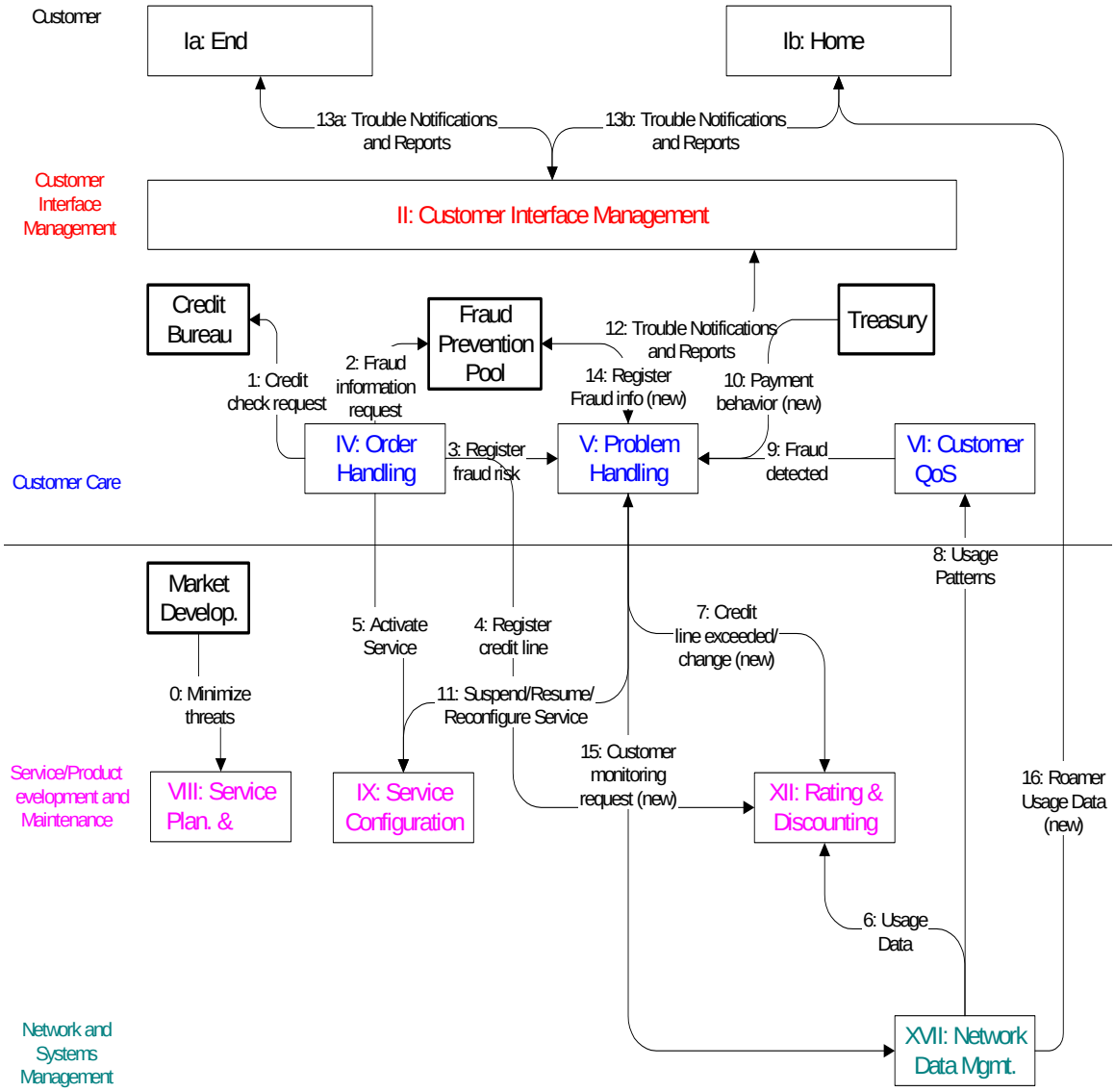
service provider when being visited by another provider's roamer. Please refer to [104] to see an example implementation with more detail.

~~Fraud and all the activities to detect and prevent fraud are quite common for most of the networks. Nonetheless it should be mentioned that two mobile network specific services: mobility and roaming make fraud detection and fraud prevention even more complicated: The mobile service provider does not know where is the "end of the wire" leading to the home of a fraudulent customer. In case of roaming the situation is even worse. The fraudulent customer uses the network facilities of another – the serving - service provider, which means that it is to a large extent out of control of the home service provider.~~

~~Typically fraud management in mobile networks (i.e. fraud detection and prevention) covers at least the following functions:~~

- ~~classification of customers according to levels of fraud risk (based on demographic and credit information);~~
- ~~revision of the fraud risk level (based on usage information, payment behaviour,... near real time or off-line);~~
- ~~detection of fraud patterns (in real time or near real time);~~
- ~~taking the appropriate actions to suspend service provision, even if the customer is using a different network than its home (the customer is roaming);~~
- ~~for visiting customers (i.e. those who are roaming) it may consult the home provider and/or international repositories (e.g. the Central Equipment Identity Register – CEIR for GSM mobile equipment).~~

~~Fraud management is present in several processes of the Telecom Operations Map. Figure 9 below shows the occurrence of fraud detection and fraud prevention functions listed above to the existing processes of the Telecom Operations Map.~~



~~Figure 9: Information flow to support Fraud Management~~

~~Fraud management functions are present in many processes of the Telecom Operations Map. What makes fraud management so difficult is the fact that it consists of many process flows segments instead of one or two continuous process flows. This is also the reason making the presentation of fraud management in the Telecom Operations Map so difficult.~~

~~Although it seems that all required functions to support fraud management exist in the Telecom Operations Map, fraud management requires the introduction of some new interfaces (marked accordingly in Figure 9) to be efficient.~~

- ~~Pre service: prevent fraud~~
  - ~~Potential threats and leaks should be analysed during Service Planning and Design and the service should be optimised to be as resistant to threats as possible.~~
- ~~Fulfilment: prevent fraud~~
  - ~~Order Handling initiates the classification of customers according to levels of fraud risk. This includes a credit check request; and~~
  - ~~A retrieval of fraud information from a fraud prevention pool (if available).~~
  - ~~The determined initial fraud risk level will be registered at Problem Handling.~~
  - ~~A credit line depending on the customer's fraud risk level will be registered at Rating & Discounting.~~

- Finally the ordered Service will be activated fully or partly depending on the fraud risk level.

- Assurance 1: detect fraud

  - Normal usage data (preferably hot billing usage data) is transferred to Rating and Discounting.

  - Rating & Discounting checks billing records for exceeding established credit lines and reports this Problem Handling (new).

- Assurance 2: detect fraud

  - Usage data/patterns are sent to the Customer QoS Management for analysis.

  - If Customer QoS Management detects a fraud then it sends an according notification to Problem handling which can decide on appropriate actions to take in order to prevent or stop fraud.

- Assurance 3: detect fraud

  - Treasury informs Problem handling about the payment behaviour of customers.

- Assurance 4: stop fraud

  - Problem Handling can decide on appropriate actions to take in order to prevent or stop fraud by reconfiguring the service; and/or

  - Contacting via Customer Interface Management

  - The Customer (either the end-customer or the home service provider in case of a visiting customer).

- Assurance 5: prevent fraud

  - Problem handling may register fraud information in the Fraud Prevention Pool.

- Assurance 6: stop roaming fraud

  - Problem handling requests the monitoring of a visiting customer on a trouble notification request of its home service provider according to the roaming agreement.

  - Network Data Management delivers the usage data to the requesting home service provider.

8.57.5 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 both 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 610 below.

8.5.1 Telecom Operations Map (TOM)

Figure 610 below 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 key to improving service quality, customer perception of service and for lowering costs.

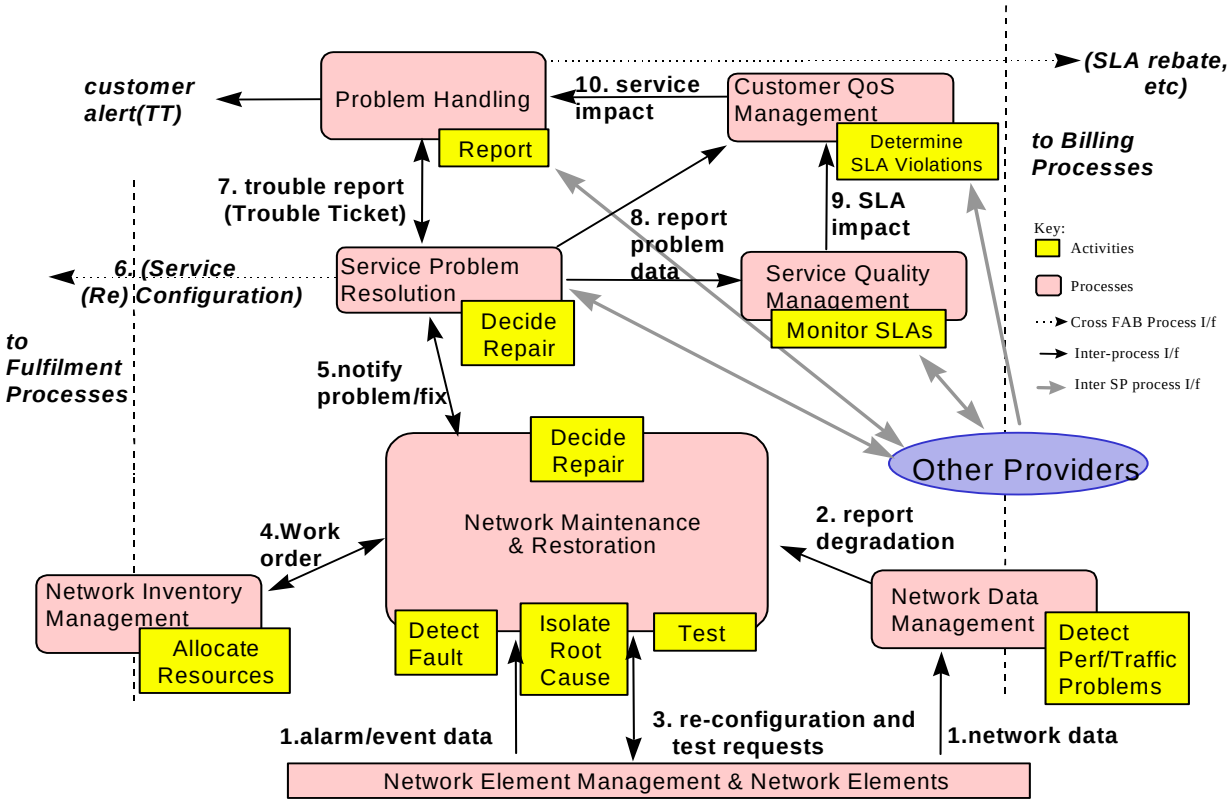


Figure 610: Service Assurance Process Flow (* imported from [100])

Note: Flow "3." has been added in this present document.

TOM assurance activities (and their associated interfaces) shown in Figure 610 above can be associated with ITU-T TMN service components from 3GPP TS 32.111-x series "3G Fault Management" [3] according to Table 1 below:

Table 1:

ITU-T TMN Service Component 3GPP 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 9 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 3G 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. 3G 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 3G TS 32.111-series [3].

~~8.5.2 General Requirements, Service Components and Functions~~

~~Fault Management service components and functions are an area well documented by existing ITU-T, ETSI and other standards. The GSM Specification GSM 12.11 (Fault Management of the Base Station System) provides a comprehensive explanation and specification of the relevant ITU-T TMN standards. This has been used as a basis for the 3GPP TS 32.111-x "3G Fault Management" [3].~~

~~3GPP TS 32.111-x [3] is based on the following service components:~~

- ~~alarm surveillance;~~
- ~~fault localisation;~~
- ~~fault correction;~~
- ~~testing.~~

~~Please refer to 3GPP TS 32.111-x [3] for complete details.~~

7.6~~8.6~~ 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~~11~~. No individual layer is dependent on any specific technology in the other one.

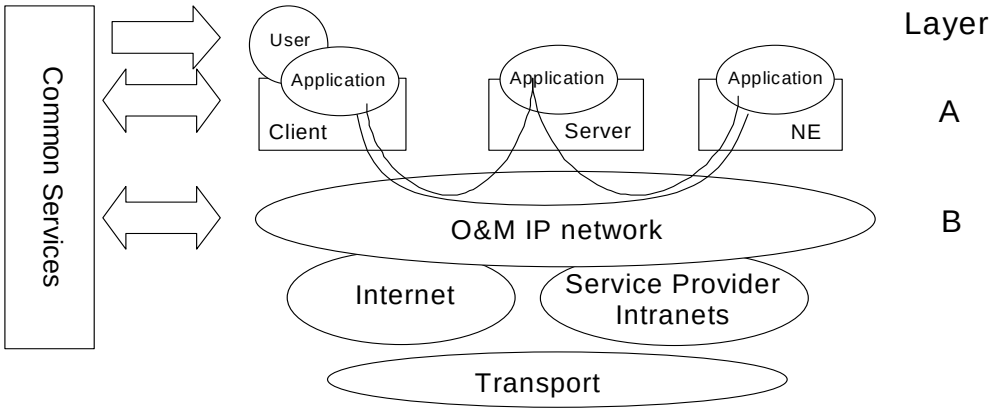


Figure 7~~11~~: Security Management Architecture

7.6.1.1~~8.6.1~~ Layer B - O&M IP Network

Some Service Providers might build their O&M IP network as a completely private, trusted network. In the normal case though, the O&M IP 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 O&M IP network is logically separated from the Internet. IP 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 RFC2401 [7]) to achieve authentication of IP hosts (servers, gateways, Network Elements) and optional encryption of O&M traffic. Note however that the secure DCN does not authenticate users.

7.6.1.2~~8.6.2~~ 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 O&M 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 O&M 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~~all~~ 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~~8.6.3~~ 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~~11~~ simply indicate the possible use of common services for Configuration Management.

7.7~~8.7~~ Software Management

7.7.1 Overview

This subclause 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~~8.7.1~~ 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~~12~~ 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~~12~~.

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.

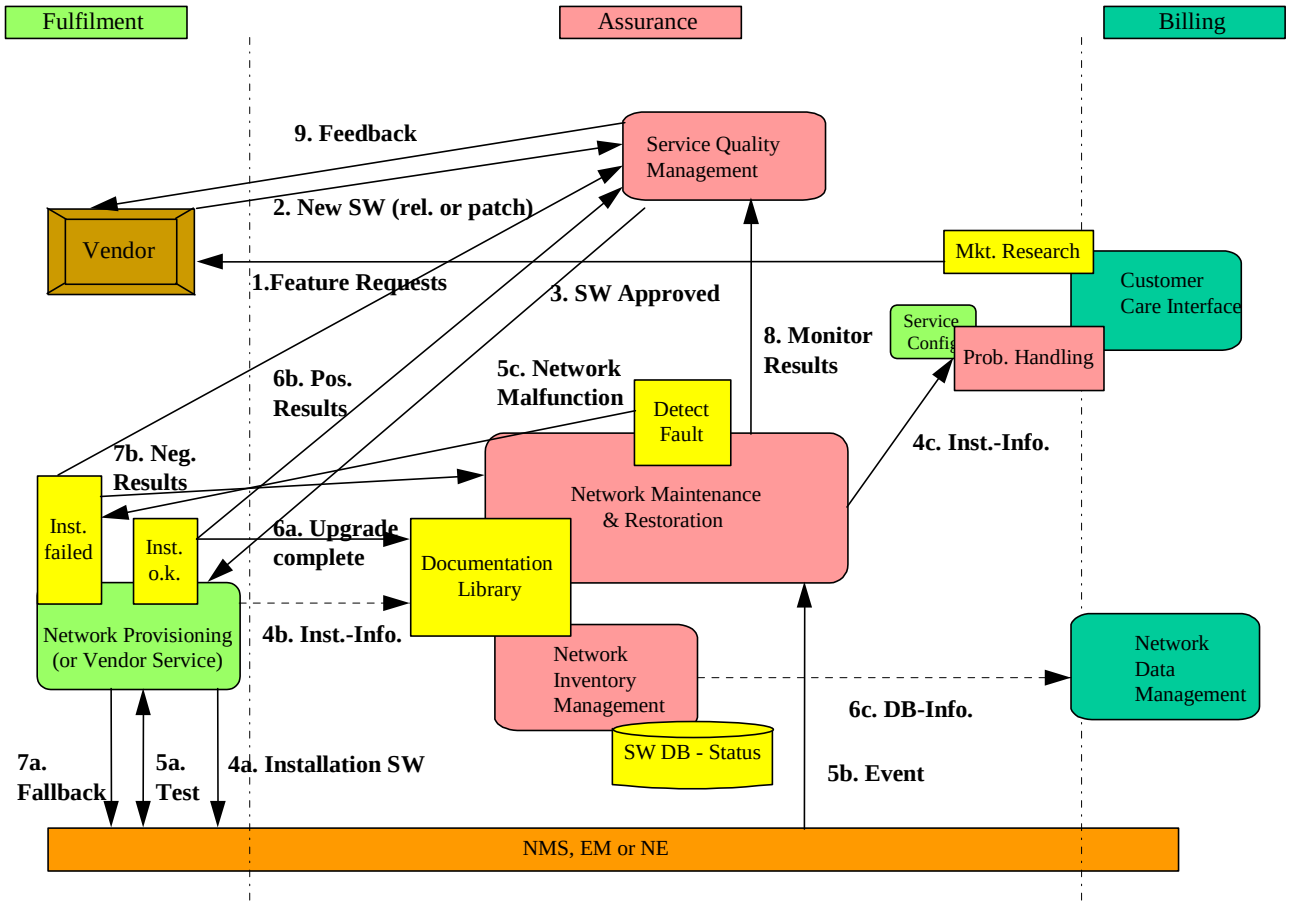


Figure 8~~12~~: Main Software Management Process

8.7.27.7.1.2 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 subclause 8.7.1.
  - Re-activation of current software.

Figure 9~~13~~ 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~~13~~.

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.

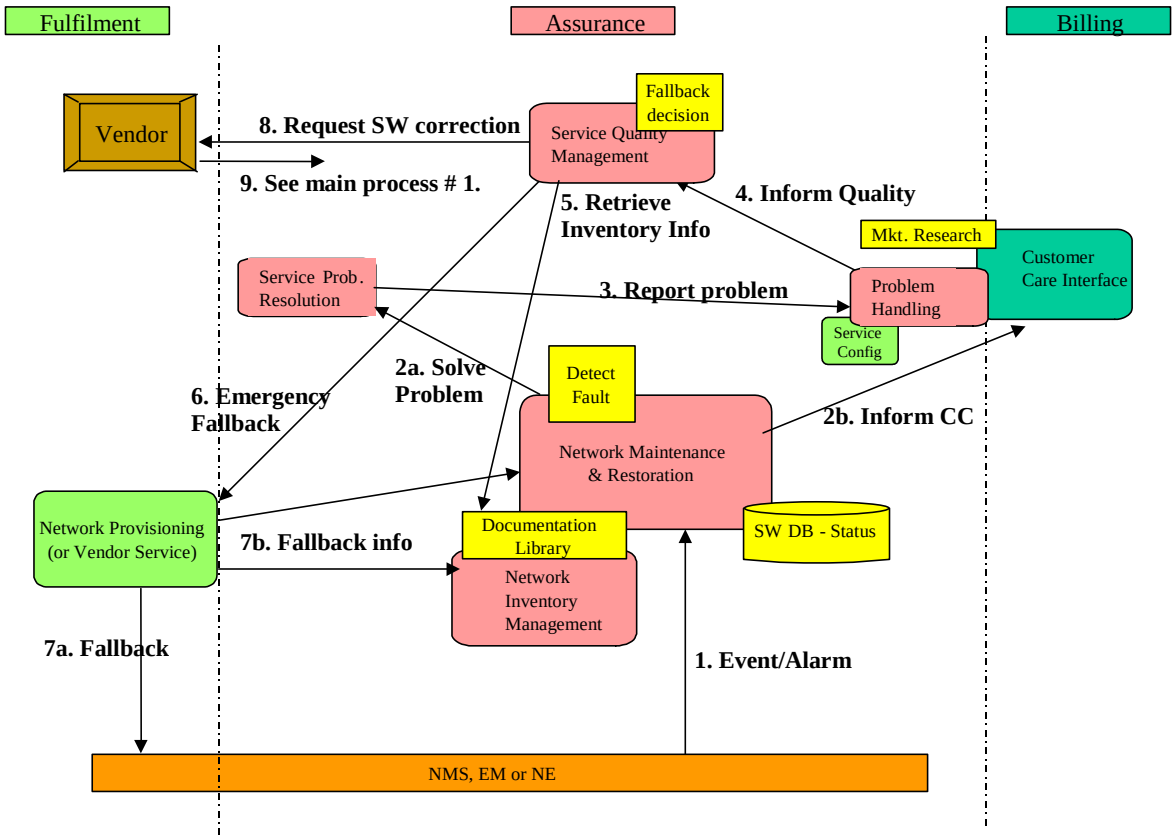


Figure 9~~13~~: Software Fault Management

7.8~~8.8~~ Configuration Management ~~(including Equipment Inventory)~~

A variety of components will make up an operator's actual implementation of a 3G network. 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 3G 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 3G TS 32.6~~xx~~00 [54].

7.9~~8.9~~ Accounting Management

3G call event data will be based on the requirements specified in 3G TS 22.115 "Service aspects; Charging and Billing" [51]. The main content of 3G call event data will be:

- Layout and formats of raw call and event data for the 3G switching nodes (circuit and packet switched);
- Data generation dependent on call states and 3GPP TS 22.115 [51] service requirements;
- Formal description of the call and event data records in ASN.1 and definition of a file transfer mechanism (FTP).

3GPP TSG-SA5 (Telecom Management) **S5-0101373**
Meeting #20, Brighton, UK, May 28th – June 1st 2001. **S5A010109**

CR-Form-v3

CHANGE REQUEST

⌘ **32.101** **CR** **012** ⌘ rev **-** ⌘ Current version: **4.0.1** ⌘

*For **HELP** on using this form, see bottom of this page or look at the pop-up text over the ⌘ symbols.*

Proposed change affects: ⌘ (U)SIM ☐ ME/UE ☐ Radio Access Network **X** Core Network X

Title:	⌘	Introduce Subscription Management
Source:	⌘	SA5
Work item code:	⌘	OAM-AR
Date:	⌘	01/06/2001
Category:	⌘	**B**
Release:	⌘	Rel4

Use one of the following categories:
F *(essential correction)*
A *(corresponds to a correction in an earlier release)*
B *(Addition of feature),*
C *(Functional modification of feature)*
D *(Editorial modification)*
Detailed explanations of the above categories can be found in 3GPP TR 21.900.

Use one of the following releases:
2 (GSM Phase 2)
R96 (Release 1996)
R97 (Release 1997)
R98 (Release 1998)
R99 (Release 1999)
REL-4 (Release 4)
REL-5 (Release 5)

Reason for change:	⌘	To introduce Subscription Management high level Requirements and framework as an informative annex to 32.101.
Summary of change:	⌘	A new clause 7.10 is added for Subscription Management.
Consequences if not approved:	⌘	Subscription Management Introduction is missing from 32.101 for Rel4.

Clauses affected:	⌘	2,8
Other specs affected:	⌘	☐ Other core specifications ⌘ ☐ Test specifications ☐ O&M Specifications
Other comments:	⌘	

2 References

[106] 3GPP TS 22.121: “The Virtual Home Environment”.

7.10 Subscription Management

Subscription Management is a feature that permits operators to provision services for a specific customer subscription. Subscription Management is related to the “Customer Care Processes” and “Service Development and Operations Processes” described above. Subscription Management is an area of Service Operation Management that sets a complex challenge for operators in their support of new or existing customers during their every day network operation.

In 2G solutions the main repository of the subscription information is in the Home Locations Register (HLR). However the management and administration interfaces that were implemented for controlling this information were proprietary to each vendor.

In 2.5G networks the HLR has been extend to form the Home Subscriber Server (HSS), which also holds information about the customer's data subscription. Again the management and administration implemented for these interfaces were proprietary.

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 customer to the provisioning, and amendment of subscription data.

The 3G environment requires more complex service delivery mechanisms than in 2G and subscription management is no longer simply an internal matter for a single operator but a capability that is achieved by linking together features across multiple operators' Operations Support Systems. The parallel trend in 2G toward Virtual Network Operators is accentuating this need.

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

7.10.1 Business Requirements

The justification for the feature “Subscription Management” is defined as follows: the network operator/service provider delivers to its subscribers various forms of services through its network operations. The delivery of such services requires a sophisticated network control that dynamically adjust the manner and the extent of the delivery based on many parameters and variables pertinent to both network and the subscriber such as, e.g., the subscriber’s static subscription limitation, the subscriber’s service-time request, the network’s temporal resource availability, etc., etc. It is clear that the subscriber’s static subscription profile data is one of the most crucial factors that determine the network’s service control mechanism.

Although the network’s service delivery mechanism of today’s network is very much automated, it still requires the operator’s OA&M involvement. One can envision in this picture two different levels of operator’s operational involvement, which both fall in the scope of service operations management:

- Operator’s management of the network service control mechanism;
- Operator’s management of the subscriber’s service profile.

Subscription Management is targeted to address the needs of the Service Provider. By providing well-thought-out standardized management procedures for subscription management, the cost of network deployment and operation will be enormously reduced because of the streamlined customer care activities.

As illustrated in the diagram below, the core part of the work will consist of the specifications that will define the interfaces and the procedures that interconnect the three points of the subscription management triangle: network

operation center (usually realized as Customer Care Center), the Customers and the network wherever the subscription profile resides (such as HLR/HSS, USIM, etc.).

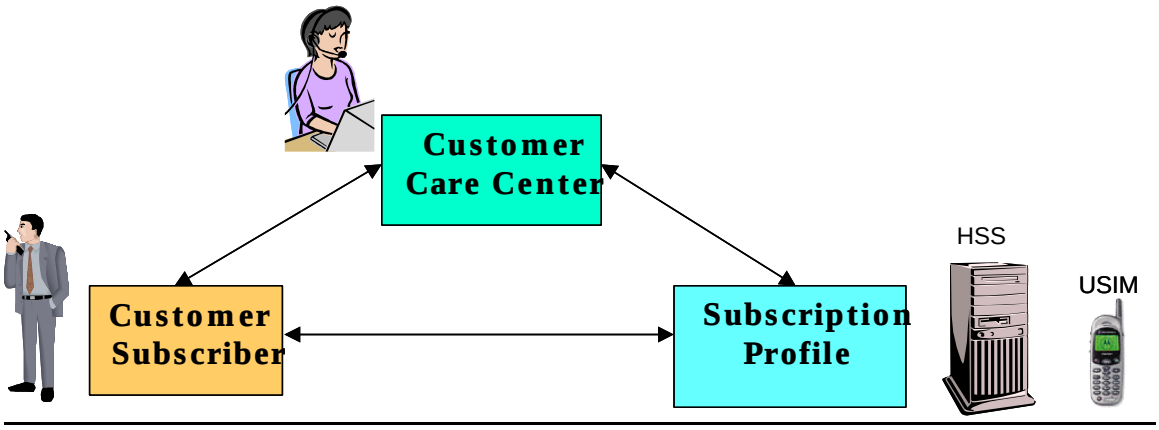


Figure 10: The Subscription Management Triangle

How the static data once provisioned into the subscription profile through the subscription management is used to determine the service control mechanism is a matter to be considered in the service control mechanism level, and it lies beyond the scope of subscription management. In this framework, any derivative forms of the subscription profile produced afterward in the network in order to facilitate the service control mechanism are considered as components defined for the service control mechanism setting and they are not visible in the subscription management realm.

7.10.2 High-level Architecture Overview

This section identifies the high level Architecture and Interfaces involved in the subscription management feature.

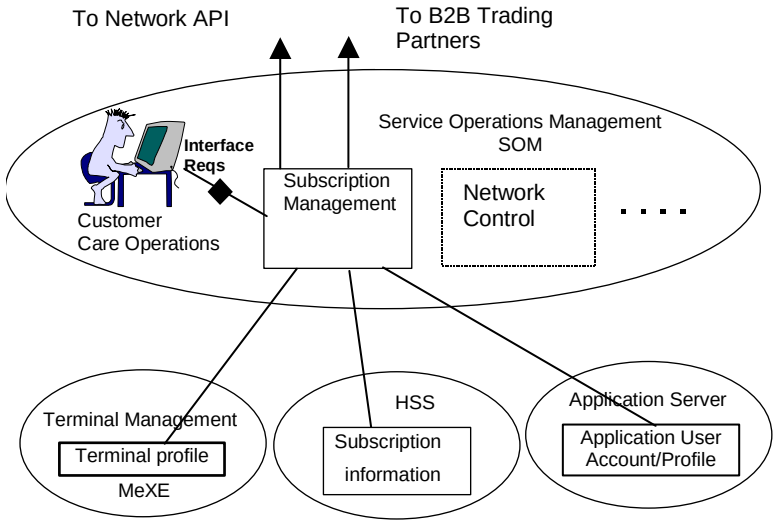


Figure 11: High Level Management Architecture

3GPP TSG-SA5 (Telecom Management) **S5-0101396**
Meeting #20, Brighton, UK, 28 May – June 1 2001 **S5A010106**

CR-Form-v3

CHANGE REQUEST

⌘ **32.101** **CR** **013** ⌘ rev **-** ⌘ Current version: **4.0.1** ⌘

*For **HELP** on using this form, see bottom of this page or look at the pop-up text over the ⌘ symbols.*

Proposed change affects: ⌘ (U)SIM ☐ ME/UE ☐ Radio Access Network **X** Core Network X

Title:	⌘	Introduction of QoS Management Annex
Source:	⌘	SA5
Work item code:	⌘	OAM-AR
Date:	⌘	01/06/2001
Category:	⌘	**B**
Release:	⌘	Rel4

Use one of the following categories:
F *(essential correction)*
A *(corresponds to a correction in an earlier release)*
B *(Addition of feature),*
C *(Functional modification of feature)*
D *(Editorial modification)*
Detailed explanations of the above categories can be found in 3GPP TR 21.900.

Use one of the following releases:
2 (GSM Phase 2)
R96 (Release 1996)
R97 (Release 1997)
R98 (Release 1998)
R99 (Release 1999)
REL-4 (Release 4)
REL-5 (Release 5)

Reason for change:	⌘	To introduce QoS Management to 32.101
Summary of change:	⌘	New informative Annex added for Quality of Service Management
Consequences if not approved:	⌘	Quality of Service Management is not part of Rel4 Telecom Management specifications.

Clauses affected:	⌘	7.1
Other specs affected:	⌘	☐ Other core specifications ☐ Test specifications **X** O&M Specifications
Other comments:	⌘	The correct section numbering of this CR is dependent on the approval of CR32.101-010_S5-010371 and CR32.101-012_S5-010373.

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 below.

The present document addresses the Functional Architecture, the Physical Architecture is addressed in 3GPP TS 32.102 [101].

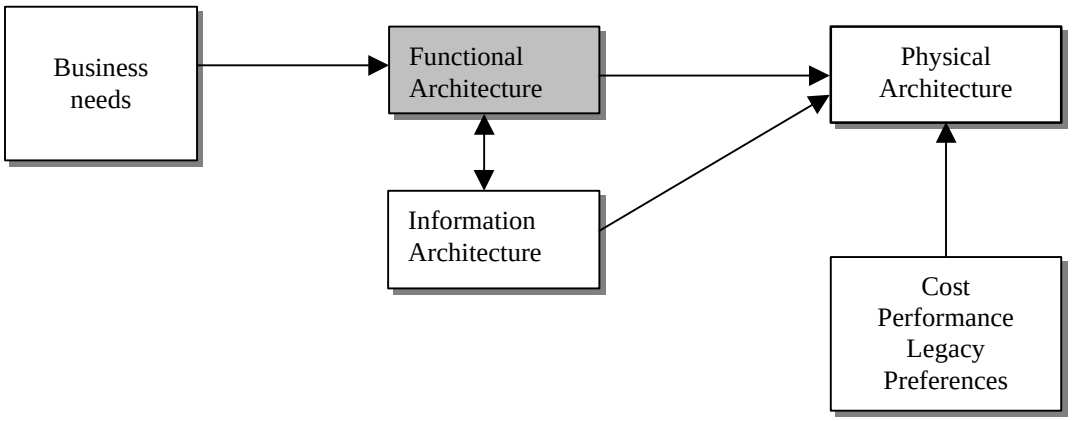


Figure 4: Architectural relationship

The present document details the UMTS Management Functional Architecture.

All UMTS 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 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)
- User equipment management

Annex D (informative): QoS Management

D.1 Overview

QoS Management, from an OAM&P perspective, in 2.5G and 3G networks 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 Managmement and QoS Provisioning and Monitoring is for future study. A conceptual breakdown of QoS Management is shown in Figure 1.

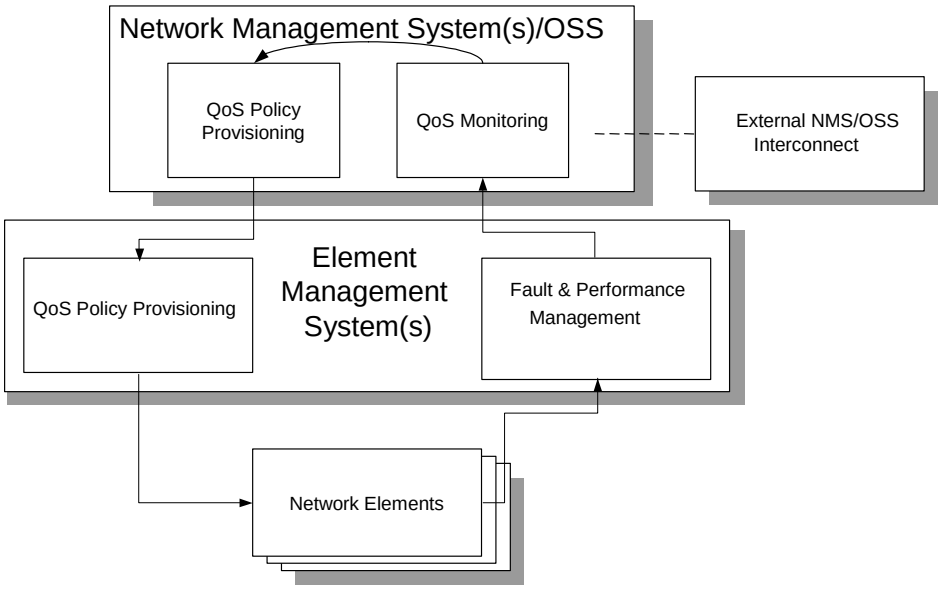


Figure 1. QoS Management

The following sections 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.1.2 QoS Provisioning

In the 2.5G and 3G networks, 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:

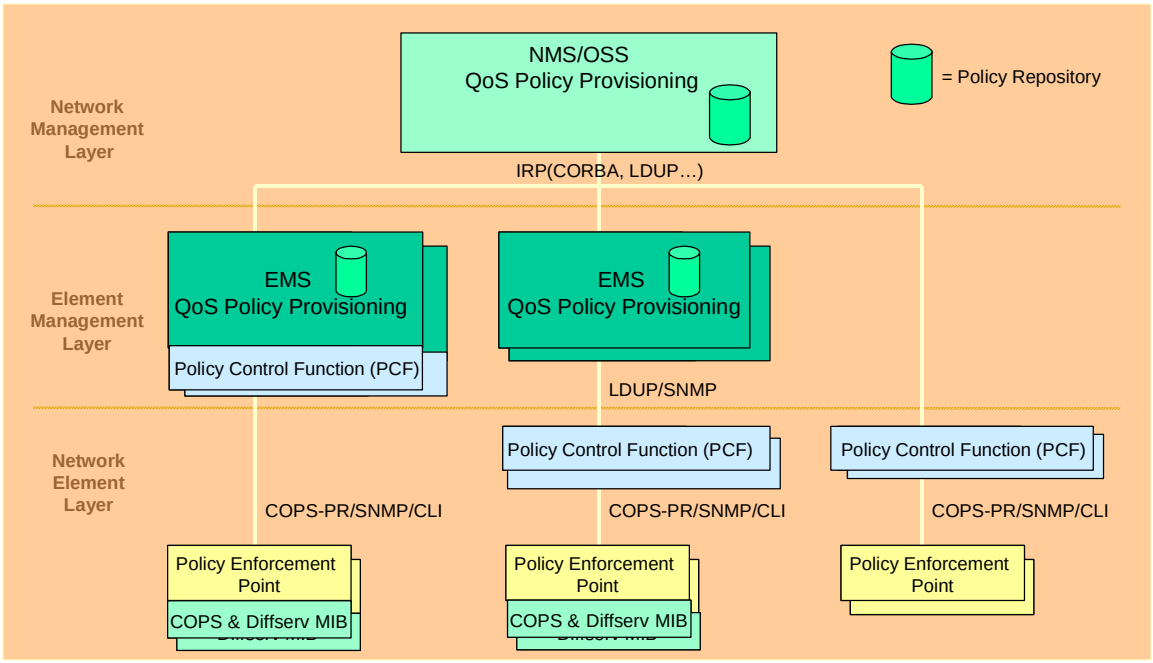
- *Automation* of management tasks.
- *Centralized* management with fewer classes of management interface.
- *Abstracted* (or simplified) management data.
- *End-to-End* provisioning of the network.
- *Consistent and uniform* provisioning across all network elements.
- *Standards-based* solution in order 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 subsections are listed in D.1.4.1. At time of writing (June 2001) there are also a significant amount of IETF Drafts available on the subject at http://www.ietf.org

D.1.2.1 Conceptual Architecture

The conceptual architecture for a policy-based QoS Management System is shown in Figure 2



Note: The 3GPP Term Policy Control Function (PCF) is equivalent to the IETF Term Policy Decision Point (PDP)

Figure 2 QoS Provisioning

The architectural components identified in figure 2 are described in the following subsections:

D.1.2.2 NMS/OSS QoS Policy Provisioning

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

The NMS/OSS 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 EMS Policy servers.
- Global policy conflict detection

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

D.1.2.3 EMS 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 EMS QoS Policy Provisioning provides the following functions:

- An optional EMS-level policy administration user interface.
- EMS-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 EMS-level policy administration user interface will be required in small networks that do not have a network-level policy provisioning OSS.

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

Finally, EMS QoS Policy Provisioning may also contain a policy decision point in those cases where there is no network element that can effectively support this function. However, this will place mores stringent requirements on the EMS such as higher availability.

D.1.2.4 Policy Control Function/Policy-Decision Point

The contents of this section fall under the responsibility of 3GPP TSG SA WG2 and will be described by specifications from that group in the Release 5 time frame.

The policy Control Function/Policy Decision Point functions as a policy server and translator for the Policy Enforcement Points under its scope of control.

It contains a policy repository as well as a translation function that converts policies from a QoS policy schema representation to a Policy Information Base (PIB), which is a representation that can be understood by the Policy Enforcement Point and loaded into the associated network element MIB.

The Policy Decision Point provides the following functions:

- Domain-specific policy repository.
- Policy distribution capability to distribute policy data to the Policy Enforcement Points
- 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 Control Function (PCF) is equivalent to the IETF Term Policy Decision Point (PDP)*

D.1.2.5 Policy Enforcement Point

The contents of this section fall under the responsibility of 3GPP TSG SA WG2 and will be described by specifications from that group in the Release 5 time frame.

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 in its MIB.
- 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

D.1.3 QoS Monitoring

QoS Monitoring in 2.5G and 3G networks 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 system and OSS 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 OSS 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 subsections are listed in D.1.4.2

D.1.3.1 QoS Monitoring Conceptual Architecture

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

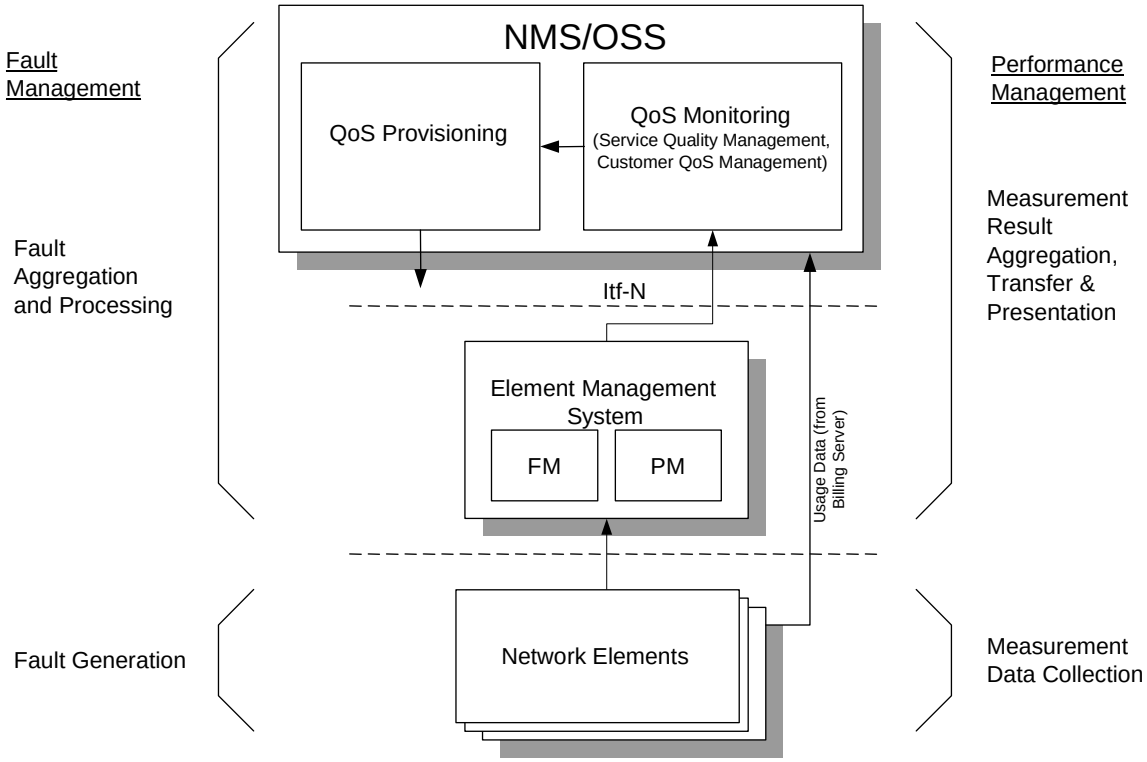


Figure 3. QoS Monitoring

The architectural components identified in Figure-3 are described in the following subsections

D.1.3.2 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 Execution Point or the Policy Distribution 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 EMS.
- 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.1.3.3 Element Management System

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

The Element Management System provides the following functions:

Performance Management

- Measurement data collection

- Measurement types. Corresponds to the measurements as defined in 3GPP TS 32.104/annex C, 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.1.3.4 Network Management System (NMS)/ Operations & Support System (OSS) Layer

From a QoS Monitoring perspective, the NMS/OSS layer is responsible for the collection and processing of performance, fault, and usage data.

The NMS/OSS 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.1.4 QoS Management References

D.1.4.1 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.1.4.2 Policy Based QoS Monitoring References

The following documents apply to QoS monitoring:

7. 3GPP TS 32.101, 3G Telecom Management: Principles and high level requirements
8. 3GPP TS 32.102, 3G Telecom Management Architecture
9. 3GPP TS 32.104: Telecommunication Management; 3G Performance Management (PM)
10. 3GPP, TS 32.005 Telecommunication Management; Charging and Billing; 3G Call and Event Data for the Circuit Switched Domain.
11. 3GPP, TS 32.205: Telecommunications Managment; Charging and Billing; 3G Charging data description for the Circuit Swirched (CS) domain.
12. 3GPP, TS 32.015 Telecommunication Management; Charging and Billing; 3G Call and Event Data for the Packet Switched Domain.
13. 3GPP, TS 32.106, Telecommunication Management; Configuration Management; 3G Configuration Management concepts and requirements.
14. 3GPP TS 32.111-1: Telecommunication Management; Fault Management; 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/

3GPP TSG-SA5 (Telecom Management)
Meeting #20, Brighton, UK, 28 May - 1 June 2001

S5-010397
S5F010102
S5A010131

CR-Form-v3

CHANGE REQUEST

⌘ **32.101** **CR** **014** ⌘ rev **-** ⌘ Current version: **4.0.1** ⌘

*For **HELP** on using this form, see bottom of this page or look at the pop-up text over the ⌘ symbols.*

Proposed change affects: ⌘ (U)SIM ☐ ME/UE ☐ Radio Access Network **X** Core Network **X**

Title:	⌘	Update the definition of IRP terminology
Source:	⌘	SA5
Work item code:	⌘	OAM-AR
Date:	⌘	01/06/2001
Category:	⌘	**F**
Release:	⌘	Rel4

Use one of the following categories:
F *(essential correction)*
A *(corresponds to a correction in an earlier release)*
B *(Addition of feature),*
C *(Functional modification of feature)*
D *(Editorial modification)*
Detailed explanations of the above categories can be found in 3GPP TR 21.900.

Use one of the following releases:

2	*(GSM Phase 2)*
R96	*(Release 1996)*
R97	*(Release 1997)*
R98	*(Release 1998)*
R99	*(Release 1999)*
REL-4	*(Release 4)*
REL-5	*(Release 5)*

Reason for change:	⌘	The IRP concept has evolved. The definition of IRP related terminology in this document is no longer in line with how the IRP concept is used in other Rel4 documents.
Summary of change:	⌘	Update the definition of the IRP terminology.
Consequences if not approved:	⌘	The IRP terminology will not be aligned with the usage of the IRP concept.

Clauses affected:	⌘	3.1 and 5.7
Other specs affected:	⌘	☐ Other core specifications ☐ Test specifications ☐ O&M Specifications
	⌘	
Other comments:	⌘	-

3.1 Definitions

Information Object : entity used to encapsulate information when modelling a network resource or a support object. The encapsulation has the form of “object classes”. It is composed of a name, attributes, relationships and may support notifications and operations. Information Object Classes are independent from the specific implementation of the interface. Information objects are the only objects used to describe Information Services.

Information Service: An Information Service describes the information related to the entities (either network resources or support objects) to be managed and the way that the information may be managed for a certain functional area (e.g. the Alarm IRP Information Service in the fault management area). Information Services can be defined for IRPs as well as for NRMs.

IRP Information Model: An IRP Information Model consists of a combination of one or more ~~an~~ IRP Information Services and ~~a~~ one or more Network Resource Models (see below for definitions of IRP Information Service and Network Resource Model).

IRP Information Service: An ~~IRP~~ Information Service for a specific IRP.~~describes the information flow and support objects for a certain functional area, e.g. the alarm information service in the fault management area. As an example of support objects, for the Alarm IRP there is the alarm record and alarm list.~~

IRP Solution Set: An IRP Solution Set contains ~~is~~ a mapping of the IRP Information Service to one of several technologies ~~(CORBA/IDL, SNMP/SMI, CMIP/GDMO, etc.)~~. ~~An IRP Information Service can be mapped to several different IRP Solution Sets. Different technology selections may be done for different IRPs.~~

Managed Object : entity used to represent information in an Solution Set. The Managed Objects (MO) are obtained as the result of a mapping exercise of Information Objects defined in IS, taking into account some engineering choices and technology specificity.

Network Resource Model (NRM): A protocol independent model describing ~~managed~~ Information O~~o~~bjects representing network resources, e.g. an RNC or NodeB. In the Information Service, the model uses Information Object Classes. In the Solution Set, the model uses Managed Object Classes.

Solution Set: A Solution Set contains a mapping of an Information Service to one of several technologies (CORBA/IDL, SNMP/SMI, CMIP/GDMO, etc.). An Information Service can be mapped to several different Solution Sets (one for each technology). Solution Sets can be defined for IRPs as well as for NRMs. Different technology selections may be done for different Information Services.

Support object : object that represents a particular capability, introduced to model a service. As an example of support object, for the Alarm IRP Information Service there is the "alarm information" and "alarm list".

5.7 Solution Set (SS) level

For ~~each~~ an IRP Information Model at the logical level there will be at least one ~~IRP~~ Solution Set defined. A~~n~~ ~~IRP~~ Solution Set is a mapping of the ~~IRP~~ Information Service to one of several technologies (for a full definition refer to subclause 3.1).

See Annex C for the valid UMTS Management IRP Solution Sets.